目录

第一章 产品概述......1

1.1 S4408MF 交换机的特性......1
1.1.1 端口特性......1
1.1.2 二层特性......1
1.1.3 三层特性......2
1.1.4 管理特性......3
1.1.5 QOS 特性......4

1.2 S4408MF 交换机的三层功能......4

1.3 S4408MF 交换机产品规格一览表......5

第二章 安装和使用......8

2.1 物品清单......8

2.2 安置方法......8

2.3 安置在桌面上的方法......9

2.4 上机架的安装方法......9

2.5 加电......9

2.6 断电......10

2.7 注意事项......10

第三章 外观介绍......11

3.1 前面板 11

3.2 后面板 11

3.3 功能模块 12
3.3.1 1000BASE-T 模块 12
3.3.2 1000BASE-SX 光纤模块 12
3.3.3 1000BASE-LX 光纤模块 13

3.4 LED 指示灯 13

第四章 管理概念 14

4.1 本地控制口管理 14

4.2 MAC 地址 14

4.3 管理信息库（MIB） 15

4.4 认证（Authentication ） 15

4.5 包转发（Packet Forwarding） 16
4.5.1 MAC 地址老化时间（Aging Time） 16
4.5.2 过滤（Filtering） 16

4.6 生成树协议（Spanning Tree Protocol） 18
4.6.1 生成树的基本概念 18
4.6.2 生成树参数 19
4.6.3 创建 STP 拓扑结构 21
4.6.4 STP 端口状态 23
4.6.5 生成树举例 24

4.7 端口聚合(Port Aggregation) 26

4.8 虚拟局域网 VLAN 27
4.8.1 802.1Q VLAN 概念 27
4.8.2 802.1Q VLAN 转发 28
4.8.3 802.1Q VLAN Tag........ 30
4.8.4 端口 VID(Port Vlan ID) 32
4.8.5 加标记和去标记 33
4.8.6 入过滤（Ingress Filtering） 34

4.9 广播风暴（Broadcast）的管理 34
4.9.1 广播风暴（Broadcast Storm） 34
4.9.2 分割广播域（Segmenting Broadcast Domains） 35
4.9.3 减少广播风暴（Eliminating Broadcast Storms） 35

4.10 组播（Multicasting） 36
4.10.1 组播组（Multicast Group） 36
4.10.2 组播地址（Multicast Addressing） 36
4.10.3 IGMP V1 和 V2........ 37

第五章 CONSOLE 接口配置 39

5.1 概括介绍 39

5.2 如何登录控制台界面 40
5.2.1 配置超级用户 41
5.2.2 配置交换机 IP 地址........ 44

5.3 CLI 命令使用说明........ 46
5.3.1 一些特殊键的使用 46
5.3.2 语法帮助 46
5.3.3 使用语法帮助补齐命令 47
5.3.4 命令帮助使用说明 48
5.3.5 常用命令 48
5.3.5.1 help 命令 48

5.3.5.2 禁止命令 disable 49
5.3.5.3 允许命令 enable 49
5.3.5.4 arp 命令 50
5.3.5.5 clock 命令 51
5.3.5.6 hostname 命令 51
5.3.5.7 保存配置命令 save 52
5.3.5.8 复位命令 reset 52
5.3.5.9 回复配置命令 resettodefaults 53
5.3.5.10 终端设置 53
baud rate 命令 53
length 命令 54
width 命令 54
5.3.5.11 ping 命令 55
5.3.5.12 ip route 命令 55
5.3.5.13 配置 tftp server 57
5.3.5.14 download 命令 58
5.3.5.15 upload 命令 58
5.3.5.16 退出命令 exit 、Ctrl+z 59
5.3.6 用户管理命令 60
5.3.6.1 添加用户命令 60
5.3.6.2 删除用户命令 61
5.3.6.3 配置密码 61
5.3.7 配置交换机端口命令 62
5.3.7.1 端口禁用命令 62
5.3.7.2 端口使能命令 62
5.3.7.3 端口风暴控制命令 63
广播风暴控制命令 63
使能广播风暴控制 63
禁止广播风暴控制命令 64
洪泛报文控制命令 65
使能洪泛报文控制命令 65
禁止洪泛报文控制命令 66
组播报文控制命令 67

允许组播报文通过命令 67
禁止组播报文通过命令 68
pause 帧收发命令 69
允许收发 pause 帧命令 69
禁止 pause 帧收发命令 70
端口流量设置命令 71
5.3.7.4 设置端口镜像命令 72
设定端口镜像状态命令 72
设置端口镜像模式命令 73
选定监听端口命令 73
显示端口镜像结果 74
5.3.8 虚拟局域网（VLAN）配置命令 74
5.3.8.1 配置 VLAN 74
创建 VLAN 命令 75
忽略 VLAN 设置并退出命令 75
应用 VLAN 设置命令 76
删除 VLAN 设置命令 76
应用 VLAN 设置并退出命令 76
清空 VLAN 设置命令 77
5.3.8.2 配置 supervlan 77
配置 subvlan 命令 79
配置 supervlan 命令 80
5.3.8.3 设置 VLAN 端口优先级命令 81
5.3.9 生成树协议 STP 配置命令 82
5.3.9.1 基于端口的生成树配置命令 82
使能基于端口的生成树协议命令 82
禁止基于端口的生成树协议命令 83
设定端口路径花销命令 83
设定端口 STP 优先级命令 86
5.3.9.2 基本 STP 设置命令 89
使能 STP 89
禁止 STP 89
设置 forward-time 命令 90

设置 hello-time 命令 91
设置报 max-age 命令 92
设置 priority 命令 93
5.3.10 认证设置 94
5.3.10.1 设置 802.1x 94
使能 802.1x 94
禁止 802.1x 94
使能端口的 802.1x 95
禁止端口的 802.1x 95
5.3.10.2 配置 radius 服务 95
配置 radius 客户端 96
配置 radius 客户端的 ip 地址 96
配置加密算法 96
配置认证端口号 97
配置计费端口号 97
显示基本 RADIUS 基本配置命令 97
配置 radius 服务器 98
查看 server 配置命令 99
5.3.11 ACL 设置 99
5.3.11.1 multicast-forwarding 命令 99
5.3.11.2 uni-forward 命令 101
5.3.11.3 packet-filter 命令 102
5.3.12 集群管理 104
5.3.12.1 ddp 命令 104
使能 ddp 106
禁止 ddp 106
配置 ddp 域名 107
设置 ddp 命令设备 107
设置 ddp 监听设备 107
显示 ddp 基本信息 108
显示 ddp 从设备 108
5.3.12.2 cluster 命令 109
使能命令设备 109

禁止命令设备 109
设置候选设备 110
禁止候选设备 110
设置独立设备状态 110
添加/删除成员设备 111
改变成员状态 112
show cluster summary 112
show cluster member 113
远程管理命令 rcommand 113
5.3.13 配置 igmp 115
5.3.13.1 设置 igmp 的版本 115
5.3.13.2 禁止 igmp 116
5.3.13.3 ip igmp snooping 命令 116
aging 116
alert 117
关闭 igmp snooping 功能 117
激活 igmp snooping 功能 118
显示 igmp snooping 设置 118
5.3.14 配置 DHCP 协议 118
5.3.14.1 关闭 DHCP relay 的功能 118
5.3.14.2 使能 DHCP relay 的功能 119
5.3.14.3 刷新命令 119
5.3.14.4 配置 DHCP server 命令 120
5.3.15 路由协议 120
5.3.15.1 使能路由协议 121
5.3.15.2 配置 OSPF 121
area 命令 121
networks 命令 122
5.3.15.3 配置 RIP 124
network 命令 124
5.3.15.4 基于 supervlan 的 OSPF 设置 125
设置认证方式 125
设置认证密钥 126

设置接口花销 127
设置 dead-interval 127
设置呼叫间隔 128
设置网络类型 129
设置接口优先级 129
设置重传间隔 130
设置传输延迟 131
5.3.15.5 基于 supervlan 的 RIP 设置 131
设置认证方式 131
设置认证密钥 132
设置接收版本 133
设置发送版本 133
5.3.16 Garp 协议 134
5.3.16.1 设置 garp 协议定时器 134
设置 join 定时器 134
leave 命令 135
leaveall 命令 136
5.3.16.2 设置静态组播组 137
5.3.16.3 gvrp 命令 138
禁止 gvrp 协议 138
使能 gvrp 协议 138
基于端口的 gvrp 139
设置接收报文的类型 139
禁止端口的 gvrp 139
使能端口的 gvrp 140
使能端口的 ingressfilter 140
禁止端口的 ingressfilter 141
pvid 命令 141
5.3.17 端口聚合管理 143
5.3.17.1 lacp 协议 143
禁止 lacp 协议 143
使能 lacp 协议 143
设置关键号 144

使能端口聚合 144
关闭端口聚合 145
设置负荷分担算法 146
5.3.17.2 静态聚合 147
禁止静态端口聚合 147
使能静态端口聚合 148
设置静态端口聚合 148

第六章 WEB 管理 150

6.1 准备工作 150

6.2 WEB 管理界面配置说明 150
6.2.1 基本配置 152
6.2.1.1 交换机信息（Switch Information） 152
6.2.1.2 交换机基本信息配置(Basic Switch Setup) 152
6.2.1.3 配置串口属性(Serial Port Setting) 153
6.2.1.4 端口配置（Port Configuration） 154
6.2.1.5 工具配置（Switch Utilities） 156
6.2.1.6 网络监视信息（Networks Monitor） 158
端口利用率（Port Utilization） 158
端口错误包统计（Port Error Packets） 159
端口数据包分析（Port Packet Analysis） 161
GVRP 状态（GVRP Status） 162
6.2.1.7 恢复出厂设置（Factory Reset） 164
6.2.1.8 存贮改变（Save Change） 165
6.2.1.9 重启系统（Restart System） 166
6.2.2 高级配置（Advances Setup） 167
6.2.2.1 生成树配置（Spanning Tree） 167
交换机生成树配置（STP Switch Settings） 167
端口生成树配置（STP Port Settings） 169
6.2.2.2 转发配置（Forwarding） 171
6.2.2.3 QOS 配置（Configure QOS） 172

6.2.2.4 端口镜像配置（Mirroring Configuration） 173
6.2.2.5 VLAN 配置（VLAN Configuration） 175
GVRP 设置........ 175
802.1Q VLAN 配置（802.1Q VLAN） 177
IEEE802.1Q 端口设置（IEEE802.1Q Port Settings） 179
6.2.2.6 链路聚合配置（Link Aggregation） 180
配置干路端口（Trunk Port Parameter） 181
配置干路策略（Trunk Group Parameter） 183
显示干路组（Trunk Show Table） 184
配置静态干路（Trunk Static Table） 185
6.2.2.7 认证配置（Authentication） 186
Radius（配置）（Radius Configuration） 186
802.1x 配置（Dot1x Configuration） 188
WEB SERVER 的配置（WEB Configuration） 190
6.2.2.8 设置多播组 192
设置静态多播 192
6.2.3 IP 路由配置（IP Routing infrastructure） 193
6.2.3.1 子网配置（Subnets） 193
6.2.3.2 配置静态路由（Static Routes） 195
6.2.3.3 SubVLAN 的配置（SubVLAN Configuration） 196
6.2.3.4 显示路由表（Routing Table） 197
6.2.4 RIP 协议（RIP） 198
6.2.4.1 RIP 配置（RIP Configuration） 198
6.2.4.2 RIP 信息统计（RIP Statistics） 201
6.2.5 OSPFV2 协议（OSPFv2） 202
6.2.5.1 OSPF 一般参数（OSPF General Paramters） 202
6.2.5.2 OSPF 区域配置（Areas） 204
6.2.5.3 OSPF 接口配置（Interfaces） 206
6.2.5.4 邻居路由信息（Neighbor Table） 209

第七章 用户常见问题........ 212

感谢您使用 TCL S4408MF 全千兆网管型以太网交换机，本手册为您提供了详细的操作说明，可以更加方便您安装和使用。

此手册若有内容变更，恕不另行通知！

第一章 产品概述

本章将简要介绍 S4408MF 的三层（Layer 3）路由交换功能，及其二层（Layer 2）和三层（Layer 3）特性。

1.1 S4408MF交换机的特性

1.1.1 端口特性

- 8 个 GBIC 插槽可热插拔高性能的 1000Base-SX/1000Base-LX/1000Base-T 功能模块；
- 提供 RS-232 控制端口(console port)，可以通过一台终端或者运行终端仿真程序的 PC 对交换机进行设置和管理；
- 提供带外 RJ-45 网口，可对交换机进行设置和管理。

1.1.2 二层特性

- 16Gbps 的交换背板
- 存储转发（Store and forward）的交换方式
- 在全双工模式下，提供 IEEE 802.3x 流量控制功能（flow control）
- 在半双工模式下，提供背压流控功能（Back-pressure flow control）
- 遵循 IEEE 802.3z 和 IEEE 802.3ab 标准
- 8K 的 MAC 地址表，自动学习（automatic learning and aging）时间为 10 秒至 1000000 秒
- 支持广播风暴（Broadcast storm）控制，可以设置广播/组播/DLF 报文的最大速率，限制广播风暴
- 支持 STP IEEE802.1D

- 支持组播功能：

  支持 IGMP Snooping，IGMP V2

- 支持端口镜像（Port Mirroring），可以将任何一个端口 GE 设置为 Mirrorred 端口或 Moniter 端口。每个端口支持以下三种 Mirror 策略或他们的混合设置：
  - 只镜像输入报文
  - 只镜像输出报文
  - 镜像所有（输入和输出）
- 支持端口聚集（Port Trunking），最多支持 6 个聚集组（trunk group），每个组中最多可以包含 8 个端口
- 支持 VLAN 功能
  - 802.1Q Tagged VLAN(其中 VLAN 1 被保留作内部使用)
  - 支持 GVRP VLAN 注册协议
  - 支持 63 个静态 VLAN 表项
  - 支持 4094 个动态 VLAN
- 支持 802.1p 优先级（Priority），提供 4 个优先队列
- 支持 RMON 功能：支持 RMON1、2、3、9 组，支持远程网络监视 MIB RFC1575
- 过滤和绑定

支持数据包过滤功能，可以允许/禁止符合某一特定特征的数据包参与交换，还可以进行限速管理。实 IP Addr - MAC Addr - Port 的绑定

1.1.3 三层特性

- 具有线速的 IP 转发性能（Wire speed IP forwarding）

- 基于硬件实现方式的（Hardware-based）三层 IP 交换（Layer3 IP switching）
- IP 数据包转发速率为（IP packet forwarding rate）线速
- 支持 2K IP 地址表（address entry table）
- 支持 RIP v1/v2
- 支持 OSPF V2
- 支持计费功能：

  S4408MF 配合 DHCP+WEB 的认证方式，可以实现基于时间的计费；
- 支持 AAA 认证功能

  支持 DHCP+WEB 认证方式

  支持 Radius Client

  支持 802.1X 模式

1.1.4 管理特性

- 提供 RS-232 控制端口（console port）
- 提供 RJ-45 用于通过一台终端或运行终端仿真程序的 PC 对交换机进行带外（out-of-band）网络管理
- 通过基于 SNMP 的软件（SNMP based software），可以进行全面的带内（in-band）配置
- 用闪存方式的软件升级设计，可以通过 TFTP 进行带内软件升级
- 内置的 SNMP 管理，即

  支持 SNMPv1/v2c

  支持 RFC1213/2233 接口管理 MIB

  支持以太网链路 MIB RFC2665

支持 OSPF v2 MIB RFC1850

支持 RIPv2 MIB RFC1724

- 支持通过 TELNET 方式进行远程网管
- 支持远程 WEB 方式网管
- 支持集群管理
- 支持 FTP/TFTP 方式的软件升级
- DHCP 功能：支持 DHCP Relay 功能，允许多个广播域共享同一个 DHCP Server
- 提供口令(Password)安全设置

1.1.5 QOS特性

- 支持 IEEE802.1p 包优先级队列
- 具有 4 个输出优先级队列

1.2 S4408MF交换机的三层功能

S4408MF交换机的三层功能可以完成传统路由器的大部分功能：

- 根据第三层（Layer 3）的信息确定转发的路径
- 通过校验和（checksum）检验三层包头（Layer 3 header）的完整性
- 检验数据包的有效期，并做相应的更新处理
- 处理或响应任何可选的信息（optional information）
- 更新 MIB(Management Information Base)中的转发统计信息
- 安全控制（security controls）

1.3 S4408MF交换机产品规格一览表

产品型号			S4408MF
端口配置	最大 GE 端口数		8 个（GBIC）
	千兆接口种类		1000Base-SX,1000Base-LX,1000Base-T
性能与功能	交换容量		16G
	3 层包转发能力*		线速
	2 层包转发能力		线速
	转发模式		存储转发
	缓冲区容量		512K
	MAC 地址表容量		8KB
	自动识别线序 MDI/MDI-X		√
	链路聚合	支持链路聚合	√
		最大 TRUNK 组	6
		最大绑定端口数	8
	堆叠	最大堆叠数量	30
		堆叠方式	菊花链
	端口镜像		√
	广播风暴控制		√
	VLAN	支持方式	端口、IEEE 802.1Q 协议
		VLAN 数量	63

		GVRP	√
	QoS	每端口最大优先级队列数	4
		支持的协议	IEEE 802.1p
		队列算法	PQ、WRR、WRRBD
		背压	√
		IEEE802.3x	√
		HOL	√
	冗余	IEEE802.1D	√
		IEEE802.3ad	√
	安全	MAC 地址过滤	√
		静态 MAC 地址表输入	√
		MAC 地址锁定	√
		IEEE802.1x	√
	三层路由协议*		RIPv1/v2、OSPFv2
	SuperVlan*		√
	ARP 代理*		√
	DHCP 中继*		√
	组播		IGMP Snooping，IGMP V2

管理	管理方式	命令行,telnet,Snmp v1/v2c、Web
	MIB	RMON(1 2 3 9)、Bridge MIB、Ether-Like MIB、MIB II
	邻居发现协议 DDP	√
	集群管理	√
	升级(TFTP)	√
物理特性	物理尺寸	442 ×240 ×43 (mm)
	工作环境	温度0 ~50 摄氏度
	功耗	60W
	电源	220V/50Hz
	重量	3Kg

注 :“ √ ” 表支持,“ * ” 表 S4408MF 所特有功能

第二章 安装和使用

本章主要介绍S4408MF 的安装和使用方法。

2.1 物品清单

打开S4408MF 的包装箱，你将看到如下物品：

♦ S4408MF 以太网交换机	一台
♦ 电源线	一根
♦ 用户手册（光盘）	一张
♦ 串口电缆	一根
♦ 安装螺钉	四只
♦ 黏性橡胶垫	四只
♦ 合格证	一张
♦ 保修卡	一张

如果发现上述物品有缺失或损坏，请立即与供货的销售商联系更换。

2.2 安置方法

请按照下述方法安置交换机：

- 放置交换机的表面（例如桌面）至少能够承受 3 千克的重量。
- 电源插座必须距离交换机 1.8 米之内。
- 确保电源线已可靠地插在电源插座上。

- 确保交换机周围留有足够的通风散热的空间，并且请不要将重物放置在交换机上。

2.3 安置在桌面上的方法

首先，将包装箱内的四个黏性橡胶垫粘贴到S4408MF 交换机背面的四个角落处，以使交换机与周围物体能够保留足够的通风空间。然后，将交换机放置于桌面上。

2.4 上机架的安装方法

S4408MF 交换机可以安装在标准的 19 寸机架内。首先，将包装箱内的上机架的配件用螺丝安装在交换机的侧板上。

然后，再用螺丝将交换机固定在19 寸机架内

2.5 加电

S4408MF 交换机的输入电压为110-240 V（50 - 60 Hz）交流电。在110V-240 V 允许输入电压范围内，S4408MF 交换机能够自动检测输入的电源值，并适应输入电压，保持正常工作。

给S4408MF 交换机加电后， 交换机前面板上的LED 状态指示灯将表现出如下状态：

- 所有 LED 指示灯将瞬间闪烁一下，这表示交换机的系统在进行复位。
- “power”指示灯在加电后将常亮，无闪烁。
- 当交换机在加载内置的程序进行自检时，“ system ”指示灯将闪烁。大约 5 秒钟之后，“ system ”指示灯将按一定频率闪烁，表示交换机已经进入稳定工作状态。

2.6 断电

当供电出现问题时，为了防止对交换机造成损坏，请将电源线从交换机上拔下。当供电恢复时，再将交换机的电源线插上。

2.7 注意事项

在使用本装置时，为避免使用不当造成设备损坏及对人身的伤害，请遵从以下注意事项：

（1） 使用前认真阅读本手册；

（2） 在清洁交换机前，应先将交换机电源头拔出， 可用湿润的布料擦拭，但不可用液体清洗；

（3） 请不要将交换机放在水边或潮湿的地方，并防止水和湿气进入交换机机壳；

（4） 请不要将交换机放在不稳定的桌子或箱子上，万一跌落，会造成严重损失；

（5） 应保持室内通风良好并保持交换机通气孔通畅；

（6） S4408MF 交换机要在正确的电压下才能正常工作，请确认工作电压与交换机所标示的电压相同；

（7） 为减少受电击的危险，在交换机工作时不要打开外壳，即使在不带电的情况下也不要自行打开。

第三章 外观介绍

本章主要介绍 S4408MF 的前面板、后面板、可选扩展模块及其 LED 状态指示灯。

3.1 前面板

在 S4408MF 的前面板上有 8 个 GBIC 插槽、1 个 RS-232 控制接口、1 个 RJ－45 端口和一些 LED 状态指示灯。

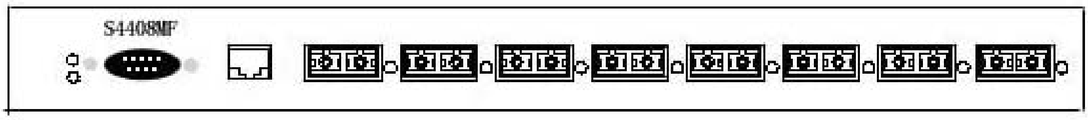


图 3-1 S4408MF 的前面板示意

- 提供了一些 LED 状态指示灯，以便监视交换机的实时工作状态（详见下文中的“LED 指示灯说明”一节）。
- 提供 1 个 RS-232 控制接口（console port），以便通过一台终端或者运行仿真终端程序的 PC 对交换机进行配置和管理。
- 1 个 RJ－45 端口可以通过 telnet 进行网络控制。
- 8 个高性能的 GBIC 插槽可以热插拔高性能的 1000Base-SX/1000Base-LX/1000Base-T 功能模块。

3.2 后面板

在S4408MF 的后面板上有一个三相的交流电源插口，支持的输入电压为100-240V（50-60Hz）

的交流电。

左侧有一些散热通风孔。是用于为交换机进行通风散热用的，以保证交换机能够正常地工作。因此，请不要挡住这些散热装置，保证交换机的两侧留有15 厘米左右的空间，以确保能够保持良好的通风散热效果。

3.3 功能模块

S4408MF 的所有功能模块都需要单独购买，出厂配置中不包括这些可选的功能模块。

3.3.1 1000BASE-T模块

- 插在前面板的扩展插槽内
- 用于连接 1000BASE-T 设备
- 支持 5 类非屏蔽/屏蔽双绞线，最大有效距离为 100 米

3.3.2 1000BASE-SX光纤模块

- 在前面板的扩展插槽内
- 用于连接 1000BASE-SX 设备，只支持全双工（full-duplex）模式
- 支持多模光纤，详细参数见下表：

光纤内径	62．5μm	62．5μm	50μm	50μm
模带宽(MHz*km)	160	200	400	500
最大有效距离（m）	220	275	500	550
最大衰减（Db）	2.33	2.63	3.25	3.43

3.3.3 1000BASE-LX光纤模块

- 在前面板的扩展插槽内
- 用于连接 1000BASE-LX 设备，只支持全双工（full-duplex）模式

3.4 LED指示灯

S4408MF 的LED 状态指示灯包括“ Power ” 、“ System ” 和“ Link ”。下面介绍各指示灯的含义。

Power：在交换机开机后，该灯将常亮（绿色），无闪烁；

System：在交换机开机自检（Power-On Self Test）时，此指示灯将瞬间闪亮，大约5 秒钟后，将按一定频率闪烁（绿色），表明交换机已经进入稳定的工作状态；

Link：Link灯位于端口的右侧，为绿色。当端口与所连接设备之间建立起正常的连接后，Link指示灯将亮，表示已经link上。

第四章 管理概念

本章主要介绍配置和管理交换机时将涉及到的一些概念和特性。

具体如何配置和管理交换机，实现这些概念和特性将在下一章中进行介绍。

4.1 本地控制口管理

本地控制口管理是指用一台终端或者一台运行终端仿真程序的PC 直接连接交换机的RS-232控制端口（console port），来对交换机进行配置和管理。这种管理方式为带外（Out-of-Band）管理方式，不需要借助网络进行通信，所以，即使网络运行不正常，也可以通过控制（console）接口对交换机进行配置和管理。

本地管理是通过终端连接操作交换机内置的控制台程序（consoleprogram），来对交换机进行管理的（详见第六章“ 使用Console接口配置交换机 ”）。

在S4408MF 交换机的内部有CPU、内存、flash等部件，其中，内存是用于存储数据的，flash用于存放配置数据、配置程序和SNMP代理固件（SNMP agent firmware）。这些部件使得交换机既可以通过控制端口（console port）进行管理和监视，也可以通过带内（in-band）网络进行管理和监视，不支持带外（out-of-band）管理。

4.2 MAC地址

交换机在出厂时还会被赋予一个唯一的MAC 地址。此MAC 地址不可以被改变，在交换机初始化界面中可以看到交换机的MAC 地址。

4.3 管理信息库（MIB）

所有管理信息和计数器都存贮于交换机内的管理信息库（Management Information Base，简称 MIB）。交换机一般使用标准的 MIB-II 管理信息库模块，因此，可以被任何基于 SNMP 的网管软件所读取。除了 MIB-II 之外，交换机还可以拥有私有的 MIB（proprietary enterprise MIB），作为补充的管理信息库。这些 MIB 也可以被网络管理系统中指定的 MIB 实体识别符(MIB Object-Identity，简写为 OID)所读取。MIB 值可以是只读的（read-only）或者可读写的（read-write）。

只读 MIB 可以是预置在交换机内部的常量（constant），也可以是随着交换机运行状态而不断变化的变量（variable）。例如，交换机的端口数量和端口的类型就是只读的常量，而统计所发生的错误的数量、或者每个端口接收并转发的数据量的计数器就是只读的变量。

可读写 MIB 通常是与用户定制（user-customized configurations）有关的变量。例如，交换机的 IP 地址、生成树算法的参数，以及端口的状态等。

如果你使用第三方的 SNMP 管理软件来管理交换机，那么你可以要求交换机厂商提供其私有的 MIB（propriety enterprise MIB）。如果你所使用的软件提供浏览和修改 MIB 的功能，那么你可以得到 MIB 的数值并改变它们（如果该 MIB 的属性允许进行写操作的话）。但是，这是比较复杂的一件事情，因为你必须知道 MIB 的 OID，并且需要一一去读取它们。

4.4 认证（Authentication ）

认证协议是为了确保 SNMP 代理（agent）和远程用户 SNMP 应用程序能够丢弃来自未被授权的用户（unauthorized users）发出的数据包。认证是采用一致性字串（community string）方式来进行身份验证的，其实现方式类似口令的安全机制。远程用户 SNMP 应用程序和 NMP 代理必须使用相同的一致性字串。SNMP 一致性字串可以在控制台程序中进行设置，最多可以输入

20 个字符。

4.5 包转发（Packet Forwarding）

交换机具有学习网络的构成情况，并根据学习到的信息进行转发数据包的能力。由于交换机仅将数据包发送给目的地址，而不是发送给网段内的所有地址，所以可以有效地减少网段内的拥塞。例如，如果端口1 收到一个欲发送给连接在端口2 上的某个站点的数据包，那么，交换机只会将此数据包发送给端口2，而不会发给任何其它端口。这个过程就是学习网络拓扑结构的过程。

4.5.1 MAC地址老化时间（Aging Time）

老化时间是一个影响交换机学习进程的参数。在老化时间内，如果地址未被使用，那么，这些地址将从动态转发地址表（由源MAC 地址、目的MAC 地址和它们相对应的交换机的端口号）中被删除。

老化时间的数值范围从10 秒~1,000,000 秒，缺省值为300 秒。过长的老化时间会导致交换机内的MAC 地址表超期，从而使交换机做出一些不正确的过滤/转发决定。但是，如果老化时间过短，会造成地址表刷新太快，大量接收到的数据包的目的地址在MAC 地址表中找不到，致使交换机只能将这些数据包广播给所有端口，这样大大地削弱了交换机
的优点。

静态转发地址表（Static forwarding entries）不受老化时间的影响。

4.5.2 过滤（Filtering）

交换机可以使用过滤数据库（filtering database）来划分网段，并控制网段间的数据通信。还可以过滤掉非法侵入的数据包。静态过滤地址表可以由 MAC 地址过滤或 IP 地址过滤方式实现。

交换机上的每个端口都对应一个碰撞域，交换机将过滤（即丢弃）那些目的地址与源地址相

同的数据包，以避免本地数据包影响网络上的正常通信。

控制非法数据包的侵入是指交换机将丢弃任何一个发往或者来自过滤地址表中的 MAC 地址或 IP 地址表的数据包。

交换机将自动处理的一些过滤:

- 动态过滤（**Dynamic filtering**）：自动学习并更新 MAC 地址表。用以将本地的数据流限定在所属的网段内。
- 依据生成树协议进行的过滤（ **Filtering done by the Spanning Tree Protocol**）：可以根据拓扑结构进行过滤，确保没有网络环路生成。
- **VLAN** 过滤：从一个 VLAN（例如，VLAN 2）中的某个成员发往另外一个 VLAN（VLAN 3）的数据包将被过滤掉。

另外在下一版本的交换机中，还增加了访问控制列表（ACL）的功能，通过 ACL 用户可以手工设定一些过滤:

- **MAC** 地址过滤（**MAC address filtering**）：手动设定需过滤的 MAC 地址，这些需过滤的 MAC 地址要么是源地址，要么是目的地址，或者两者都是。符合该过滤条件的数据包将被交换机丢弃。
- **IP** 地址过滤（**IP address filtering**）：手动设定需过滤的 IP 地址（交换机必须工作在 IP 路由模式），这些需过滤的 IP 地址要么是源地址，要么是目的地址，或者两者都是。符合该过滤条件的数据包将被交换机丢弃。
- 应用层端口号过滤（**ports filtering**）：手动设定需过滤的应用端口号，这些需过滤的应用端口要么是源端口，要么是目的端口，或者两者都是。符合该过滤条件的数据包将被交换机丢弃。

4.6 生成树协议（Spanning Tree Protocol）

IEEE 802.1D 生成树协议（Spanning Tree Protocol）允许网络上存在环路时，自动断开环路连接。当检测到交换机间存在多条连接时，将只启动最主要的一条连接，而将其他连接都阻塞掉，将这些连接变为备用连接。当主连接出现问题时，生成树协议将自动起用备用连接接替主连接的工作，不需要任何人工干预。一旦生成树协议被设置好并启动，将会自动建立主连接，并自动阻塞其余形成环路的连接。

这种网络自动重构的功能，使得网络上的用户能够最大限度地与网络保持正常的连接。但是，生成树算法较复杂，所以，建议最好在充分研究理解其之后，再更改其一些设置。请仔细阅读并理解下述内容之后，再去更改交换机上的生成树的默认设置。

S4408MF 交换机上的生成树提供如下功能：

- 自动重建生成树，以补偿发生的连接故障，增加或删除生成树中的组成成员。
- 重构生成树，不需要任何人工干预。

4.6.1 生成树的基本概念

根桥（Root Bridge）：具有最小桥标志级数的（lowest Bridge Indentifier）交换机是根桥（Root Bridge）。当然，你希望根桥是环路中所有交换机中最好的一台交换机，以保证能够提供最好的网络性能和可靠性。

桥标志级（Bridge Indentifier）：桥标志级是桥的优先级和交换机的 MAC 地址的综合数值，其中桥的优先级是一个用户可以设定的参数。例如，“ 4 00 80 00 01 00 02 ”中的 4 是桥的优先级，“ 00 80 00 01 00 02 ”是桥的 MAC 地址。交换机的桥标志级数越低，则交换机的优先级越高，这样可以增加其成为根桥的可能性。

指定桥（TPESignated Bridge）：在每个网段中，到根桥的路径开销最低的（lowest Root Path

Cost）桥将成为指定桥，数据包将通过它转发到网段。一旦所有的交换机具有相同的根路径开销（Root Path Cost），那么优先级最高的交换机才能被定为指定桥。

根路径开销（Root Path Cost）：从根到达一个桥的成本开销成为该桥的根路径开销。一台交换机的根路径开销的计算方法是将从根桥到达此网桥通路中沿途的端口路径开销数字相加。

桥的优先级（Bridge Priority）：是一个用户可以设定的参数，设定的值越小，优先级越高。交换机具有教高的优先级，才能成为根桥。

根端口（Root Port）：每台交换机都有一个根端口，这个端口到根桥的开销路径最低。一旦多个端口具有相同的到根桥的路径开销，那么具有最低的端口标志级别的端口才能成为根端口。

指定端口（TPESignated Port）：将网段连接到其指定桥的单一非阻塞端口。

端口优先级（Port Priority）：数值越小，端口的优先级就越高，具有较高优先级的端口，才可能成为根端口。

路径开销（Path Cost）：这是一个可变的参数，它将随着生成树的设定值的变化而变化。依据 STA 的默认参数值，每个 1000Mbps 网段有一个指定的路径开销值为 4, 100Mbps 网段的路径开销为 19, 10Mbps 网段的路径开销值为 100。

4.6.2 生成树参数

用户可以根据需要修改生成树的参数，但建议最好使用出厂时的默认值设置。除非确实需要对出厂默认值进行变动时，再去改动默认值。用户可以改动的生成树参数有以下几个：

桥优先级（Bridge Priority）：数值范围从“ 0 ”到“ 65535 ”，0 的优先级最高。

呼叫时间（Bridge Hello Time）:数值范围从“ 1 ”秒到“ 10 ”秒，是指根桥向所有交换机发出 BPDU 数据单元包时的时间间隔，以告知其它交换机它是根桥。如果你的交换机还未是根桥时为其设置了呼叫时间，一旦你的交换机成为根桥，该呼叫时间就会派上用处。

注意：呼叫时间不能大于桥的老化时间，否则将出现错误信息。

最大的桥老化时间（Bridge Max.Age）：数值范围从“ 6 ”秒到“ 40 ”秒。如果再超出最大老化时间后，还没有收到根桥发出的 BPDU 数据包，那么在允许的情况下你的交换机将充当根桥向其它所有的交换机发送 BPDU 数据包。如果该交换机确实具有最小的桥标志级数，那么它将随之成为根桥。

桥转发时延（Bridge Forward Delay）：数值范围从“ 4 ”秒到“ 30 ”秒，是指交换机的端口从阻塞状态变为转发状态所用的监听时间。

端口优先级（Port Priority）:数值范围从”0”到“ 255 ”，数值越小，该端口就越可能成为根端口。

当用户欲变动生成树参数时，请一定记住下述公式：

最大的桥老化时间<=2×（桥转发时延－1 秒）

即：Max.Age <=2×(Forward Delay-1)

最大的桥老化时间>＝2×（呼叫时间＋1 秒）

即：Max.Age>=2×（Hello Time+1）

生成树参数	设置值	效果	备注
桥优先级（Bridge Priority）	数值越小，优先级越高	增加成为根桥的机会	如果交换机用于大型的工作组级的网络中，那么，尽量避免使用。
呼叫时间（Hello Time）	1 – 10 秒	如果不是根桥，那么，没有任何影响。	不要大于最大老化时间（Max. Age Time）。
最大老化时间（Max. Age Time）	6 – 40 秒	如果没有收到BPDU 数据包，那么，竞争成为根桥。	尽量不要选用较小的数值，以免不断不必要地重设根桥。
转发时延（Forward Delay）	4 – 30 秒	数值越高，时延越长。	Max. Age • 2 x (Forward Delay - 1) Max. Age • 2 x (Hello Time + 1)
端口级生成树参数（Port Level STA parameters）			
Enable / Disable	Enable / Disable	Enable / disable	将某个端口设置为Disable，以隔离故障或者出于安全的目的。
端口优先级（Port Priority）	数值越小，优先级越高。	增加成为根端口的可能性。	

表格 1 生成树端口状态

4.6.3 创建STP拓扑结构

为了达到稳定的网络拓扑，生成树将用到下述信息：

- 唯一的交换机标识符（unique switch identifier）
- 交换机上的每个端口到根端口的路径开销（path cost）

- 端口标识符（port identifier）

生成树协议在交换机间进行通信时使用的是 BPDU（Bridge Protocol Data Units）。每个 BPDU 中包含如下信息：

当前根交换机（root switch）的唯一标识符。

从发送端口（transmitting port）到根（root）的路径开销（path cost）。

发送端口（ transmitting port ） 的端口标识符（ port identifier）。

交换机通过发送 BPDU 来进行通信并构建生成树拓扑，连接到 LAN 的所有交换机都将接收 BPDU。交换机并不直接转发 BPDU，但是接收 BPDU 的交换机会计算 BPDU，如果网络拓扑发生改变，就会发出一个 BPDU。

利用 BPDU 进行的交换机间的通信将导致如下结果：

一台交换机被选为根交换机（root switch）

- 为每台交换机计算到根交换机最短的距离（ shortest distance）
- 选出指定交换机（TPESignated switch），该交换机是最靠近根交换机（root switch）的交换机，数据包将通过该交换机转发给根交换机。
- 选出每台交换机上的一个端口，该端口是该交换机到根交换机的最佳路径。
- 选出生成树内的所有端口。

如果所有启动生成树协议的交换机都使用缺省的设置值，那么，具有最小 MAC 地址的交换机将成为根交换机（root switch）。通过提高交换机的优先级（数值越小），生成树协议可以将其强制选定为根交换机。

当生成树协议使用缺省参数值时，源站点和目的站点之间的路径未必是最理想的。例如，一个到某个端口的高速率的连接可能使得根端口发生改变，因其数值优于了当前的根端口。因为生

成树追求的目标就是根端口应具有最快的连接。

4.6.4 STP端口状态

BPDU 在网络上传输是需要时间的，这种传播时延能导致拓扑改变，一个端口的状态从阻塞状态变为转发状态，从而产生短暂的网络环路。这样，其他端口在开始转发数据包之前，必须等待新的网络拓扑信息。转发时延（forward delay timer）被用于网络拓扑发生变化时，用以稳定网络拓扑。另外，STP 定义了一系列的状态，以确保网络拓扑发生变化后能够建立起新的稳定的网络拓扑。

交换机上的端口在启动 ***STP*** 协议后，存在的五种状态：

- 阻塞（Blocking） – 该端口被阻塞，不可以转发或接收数据包。
- 监听（Listening） – 该端口正在等待接收 BPDU 数据包，BPDU 可能告知该端口重新回到阻塞状态。
- 学习（Learning） – 该端口正在向其转发数据库中添加地址，但是，并不转发数据包。
- 转发（Forwarding） – 该端口正在转发数据包。
- 失效（Disabled） – 该端口只是相应网管消息，并且必须先转到阻塞状态。

端口可以转换的状态：

- 从初始化（交换机启动）到阻塞状态（blocking）
- 从阻塞状态（ blocking ）到监听（ listening ）或失效状态（disabled）
- 从监听状态（ listening ）到监听（ learning ）或失效状态（disabled）
- 从监听状态（listening）到转发（forwarding）或失效状态（disabled）
- 从转发状态（forwarding 到失效状态（disabled）
- 从失效状态（disabled）到阻塞状态（blocking）

当启动STP 后，网络上的每台交换机上的每个端口都将经历阻塞状态，然后，转换为监听状态或学习状态。如果STP 设置正确，那么，每个端口都将稳定地工作在转发或阻塞状态。
任何数据包（除了BPDU 数据包之外）都不会被转发或接收，直至端口进入转发状态。

4.6.5 生成树举例

在一个环路中有三个桥（或三台交换机），如图5-1 所示。在此例中，如果不使用生成树技术，你可以预见到可能发生的一些网络故障。例如，如果桥A 向桥B 发出一个广播包，那么，桥B 将把此数据包广播给桥C，而桥C 又会将此数据包广播回给桥A。随后会一直将如此反复，广播包将会在这个环路中被循环往复地传递，从而导致严重的网络故障。

为了避免网络环路的发生，可以如图5-2 所示采用生成树（STP）来解决。生成树将阻断桥B 与桥C 之间的连接，以打破环路的形成。生成树算法将根据计算出来的各桥和端口之间的数值，来决定断开哪一条连接。现在，如果桥A 向桥C 发出一个广播包，那么，桥C 将在端口2处将此数据包丢弃，那么此广播将结束。

生成树的算法较复杂，所以，建议尽量不要改动其出厂默认设置值。生成树将自动任命根桥/根端口，并避免环路的形成。

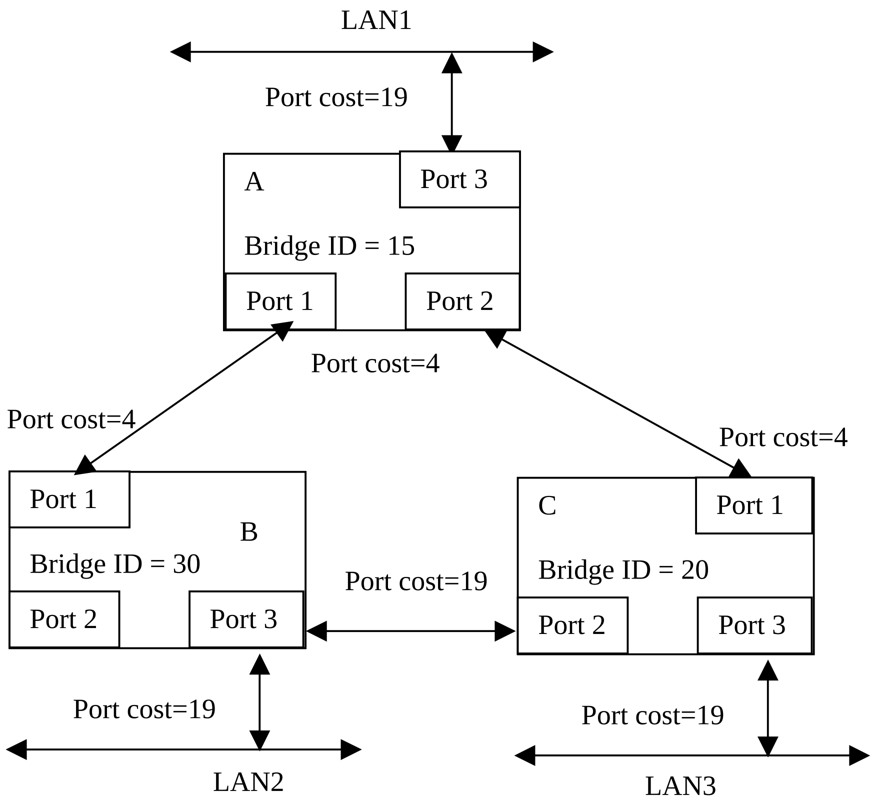

LAN1
Port cost=19
A
Port 3
Bridge ID = 15
Port 1
Port 2
Port cost=4
Port cost=4
Port cost=4
Port 1
B
Bridge ID = 30
Port 2
Port 3
Port cost=19
C
Port 1
Bridge ID = 20
Port 2
Port 3
Port cost=19
LAN2
Port cost=19
LAN3

图 4—1 应用 STP 之前

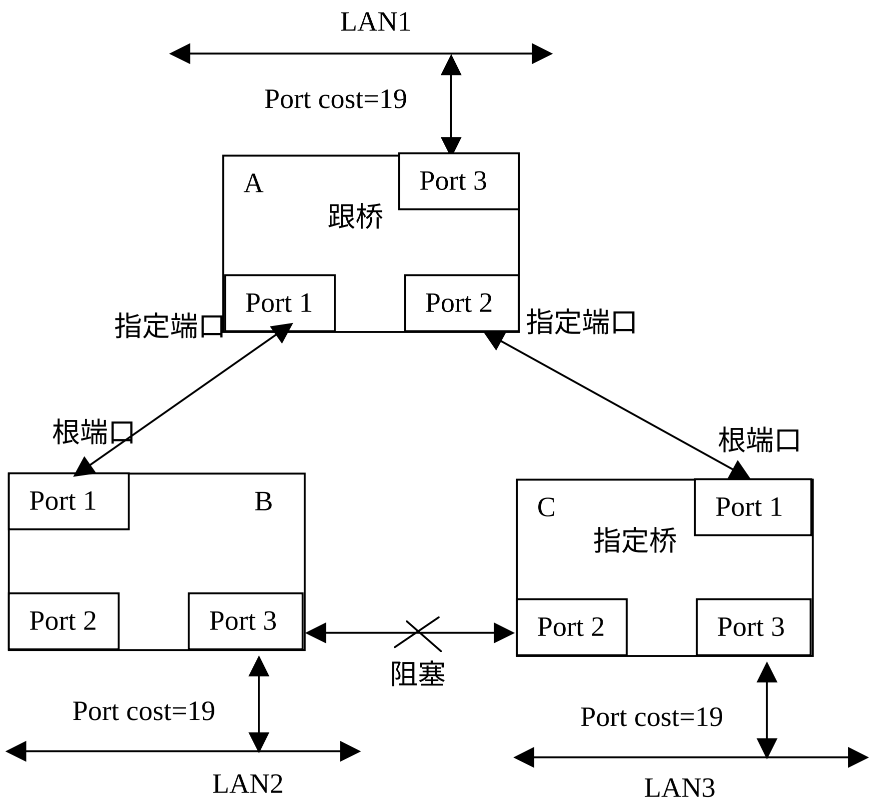


图 4－2 应用 STP 之后

4.7 端口聚合(Port Aggregation)

端口聚集通常被用于将多个端口聚集在一起，从而形成一个高带宽的数据传输通道。交换机将把端口聚集内的所有端口看作一个端口。在组成端口聚集的端口中，将有一个端口被指定为主端口（master port）。

由于干路中的所有成员需以相同的方式工作，所以，所有对主端口（master port）进行的设

置，都将被同样作用到所有成员端口上。这样，当你需要对端口聚集中的端口进行设置时，可以仅对主端口进行设置即可。

S4408MF 交换机上可以最多设置 6 个端口聚集组，端口聚集组可以包含 2 到 8 个端口。

交换机将把端口聚集组中的所有端口看作一个端口，这样，聚集端口组将不会被生成树（STP）阻断。

4.8 虚拟局域网VLAN

虚拟局域网（Virtual Local Area Network，简写VLAN)是一种逻辑上的网络拓扑设置，而不是物理上的网络设计。VLAN 可以将网络逻辑地分割成数个不同的广播域，这样，数据包只能在VLAN 内进行转发。较有代表性的说明就是一个VLAN 就类似一个子网（subnet）。VLAN 可以通过有效分割（保存带宽）的方式，提高网络的整体性能，并且可以提高数据传输的安全性。

VLAN 是将一些网络节点逻辑地组合在一起，而不是将其物理位置集中在一起。在一个VLAN 中的网络节点可以随时相互通信，无论它们当时处在网络上的物理位置在何处。逻辑上来说，一个VLAN 等于一个广播域，因为广播数据包只在VLAN 内传播，不会传播到VLAN 之外。

4.8.1 802.1Q VLAN概念

S4408MF 支持IEEE 802.1Q VLAN ，该VLAN涉及到以下概念：

- 加标记（**Tagging**） - 将 802.1Q VLAN 信息添加到数据包的包头（header）中的动作。
- 去标记（**Untagging**） - 将 802.1Q VLAN 信息从数据包的包头（header）中去掉的动作。
- 入端口（**Ingress port**） - 交换机上的端口，数据包从该端口进入交换机，在此必须判断其VLAN 属性。
- 出端口（**Egress port**） - 交换机上的端口，数据包从该端口流出交换机，传送到其他交换机

或网络节点站点，在此必须确定数据包的标记（tag）属性。

VLAN 允许将网络分成数个网段，以减小广播域的范围。所有数据包（包括从未知源地址来的广播包、组播包和点播包）都只能在本地VLAN 中进行传送。

VLAN 还可以为你的网络提供一定的安全性。IEEE 802.1Q VLAN 只能在其VLAN 成员端口范围内传送数据包。

任何一个端口都可以被设置*tagging* 或*untagging*。IEEE 802.1QVLAN 的*untagging* 特性使得无法识别VLAN 标记（tag）信息的交换机也能与S4408MF 在一起工作。而*tagging* 特性可以使VLAN 信息在整个网络中传递。

IEEE 802.1Q VLAN 的主要特征如下：

- 通过过滤（filtering）分派数据包（packet）到 VLAN。
- 假设存在一个全局生成树（a single global spanning tree）。
- 采用明确的一级（one-level tagging）加标记策略（tagging scheme）

4.8.2 802.1Q VLAN转发

- 进入规则（Ingress rules） – 属于一个 VLAN 的接收到的数据帧（received frame）的分类规则。
- 端口间的转发规则（Forwarding rules between ports） – 确定是过滤数据包还是转发数据包。
- 发出规则（Egress rules） – 确定数据包是加标记传送，还是去标记传送。

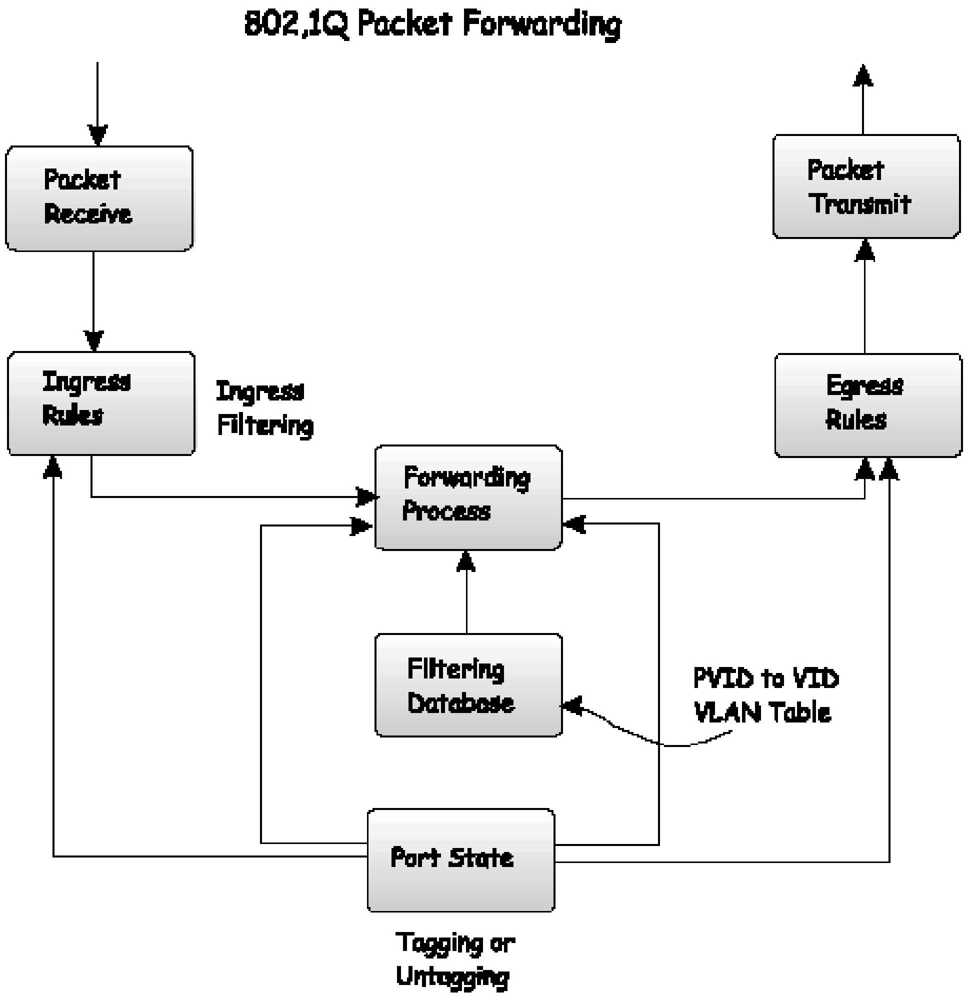


图 4－3 IEEE 802.1Q 数据包转发

4.8.3 802.1Q VLAN Tag

图5-4 示意出了802.1Q VLAN 标记（tag）的原理。在源MAC 地址的后面，将插入4 个字节（ octet ） 的标记（ tag ） 。当数据包的EtherType 字段为0x8100 时，就表示数据包中携带有IEEE802.1Q/802.1p 标记（tag）。在标记（tag）中除了包含上述2 个字节（octet）之外，还有3 个比特（bit）的优先级信息、1 个比特的CFI信息（Canonical Format Identifier，用于压缩Token Ring 数据包，以使其可以在以太网主干内传输），及12 比特的VLAN ID (VID)。3 个比特的优先级信息为802.1p 准备的，而VID 是VLAN 的标识符（identifier），是为802.1Q 准备的，因为VID 长度有12 个比特，所以，可以设置4094 个VLAN。

将标记（tag）插入到数据包的包头内后，数据包将增长4 个字节（octet）。原来数据包中包含的信息都将保持不变将标记（tag）插入到数据包的包头内后，数据包将增长4 个字节（octet）。原来数据包中包含的信息都将保持不变。

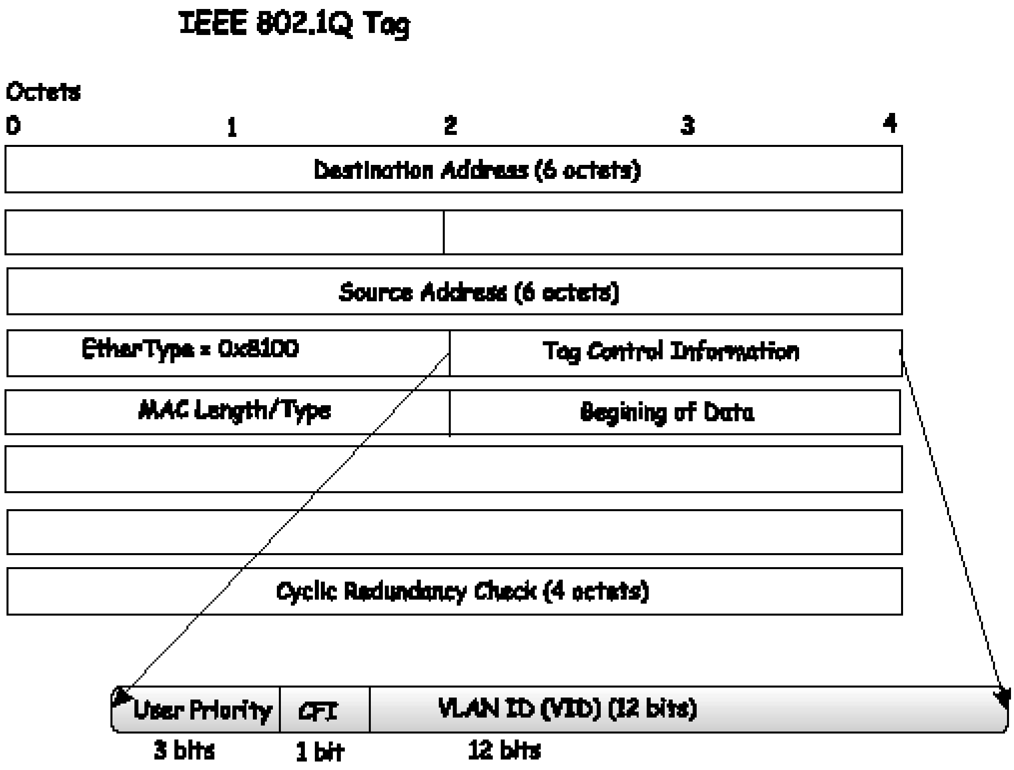


图 4－4 IEEE802.1Q 标记

EtherType 和VLAN ID 插在源MAC 地址（MAC source address）的后面，但是，位于原有的EtherType/Length 或Logical Link Control 之前。因现在数据包的长度比原来的略长， 所以，CRC(CyclicRedundancy Check)必须重新计算。

4.8.4 端口VID(Port Vlan ID)

被标记过的（即携带有802.1Q VID 信息的）数据包将从一台具有802.1Q 功能的设备传送到另一台具有802.1Q 功能的设备，在传递期间VLAN 信息保持不变。只要网络上的所有设备都支持802.1Q，就可以使802.1Q VLAN 可以延伸至整个网络。

但是，并不是网络上的所有设备都支持802.1Q。这些不支持802.1Q的设备被称为是*tag-unaware*，而支持802.1Q 的设备称为是*tagaware*。

在出现802.1Q VLAN 之前，更常使用的是基于端口（port-based）的VLAN 和基于MAC 地址（MAC-based）的VLAN。这些VLAN 依据端口VLAN ID(Port VLAN ID ，简写PVID) 信息进行数据包转发。从某个端口接收到的数据包将被赋予该端口的PVID 值，然后，将该数据包转发到其目的地址（查看交换机的转发地址表）。如果接收数据包的端口的PVID 与将转发该数据包的端口的PVID 不同，那么，交换机将丢弃此数据包，不进行转发。

在交换机内，不同的PVID 意味着不同的VLAN。请注意：在不存在路由器的情况下，两个VLAN 之间是不能相互通信的。

交换机上的每个物理端口都有一个PVID，同时802.1Q 端口也会被赋予一个PVID。如果交换机上未定义VLAN，那么，所有端口都将属于一个缺省的VLAN，其PVID 都等于1。这样，接收到的未加标记的（Untagged）数据包将被赋予接收端口的PVID 值，是否转发的决定将依据该PVID 进行确定。已携带有标记信息的（Tagged）数据包将根据其标记的VID 信息来决定是否进行转发。已有标记的数据包也将被赋予一个PVID，但是，并不是根据此PVID 来决定是否转发该数据包，而是根据其VID 信息来进行判定。支持标记功能的交换机Tag-aware switches）必须具有能够建立交换机内各端口的PVID 与网络上的VID 之间关系表的能力。交换机将把数据包中的VID 与将传送该数据包的端口的VID 进行比较，如果两个VID 不同，那么，交换机将丢弃此数据包，不进行传送。由于针对未加标记的数据包存在着PVID，对加过标记的数据包存在着VID，所以，具

有标记功能的交换机和不具有标记功能的交换机可以在同一个网络中共存。

交换机上的一个端口只可以有一个PVID，但是，可以有多个VID，（也就是是说一个端口可以属于多个VLAN）。交换机内有VLAN 表（VLAN table）可以用于存储VID 信息。

注: *802.1Q VLAN 需要创建一个包含所有端口的缺省VLAN ，这将赋予所有端口的PVID =1 ，并将PVID 对应出相应的VID 。实际上，该缺省VLAN 是交换机的出厂设置之一，所有端口都将被初始化为PVID = 1 。*

因为网络上的有些设备不具有标记功能（tag-unaware），所以，在数据包被传送之前，具有标记功能的（tag-aware）设备上的端口必须做出决定将传送出去的数据包是否应加上一个标记（tag）？如果传送端口连接的是一台不支持标记功能的设备，那么，数据包就不必加上标记。反之，如果传送端口连接的是一台支持标记功能的设备，那么，数据包就必须加上标记。

4.8.5 加标记和去标记

802.1Q 交换机上的每个端口都将被设置为*tagging* 或*untagging* 。具有tagging 功能的端口将把VID、优先级（priority）和其他VLAN 信息插入到所有流入和流出该端口的数据包的包头中。如果数据包事先已被标记过，那么，端口将不对数据包进行变更，这样，将保持其VLAN信息不变。这样，标记中的VLAN 信息将被其他802.1Q 设备所使用，以确定数据包是否应被转发。

具有untagging 功能的端口将把所有流入和流出该端口的数据包中的802.1Q tag 信息去掉。如果数据包中不含有802.1Q VLAN tag，那么，端口将不对数据包进行变更。这样，untagging 端口接收和转发的所有数据包中都将不带有802.1Q VLAN 信息。请注意：PVID 是仅限于交换机内部使用的。Untagging 功能是用于将数据包从具有802.1Q功能的网络设备传递到不802.1Q 功能的网络设备的。

4.8.6 入过滤（Ingress Filtering）

入端口（*ingress port*）是交换机上的这样一个端口——数据包从该端口流入交换机，并且必须在该端口确定其VLAN 属性。如果端口的入站过滤（ingress filtering）被设置为生效（enabled），那么，交换机将检查数据包包头中的VLAN 信息（如果存在的话），并决定是否转发该数据包。

如果数据包中包含VLAN 信息（即被加过标记），那么，入端口首先判定入端口本身是否是标记VLAN 的成员端口。如果不是，那么，该数据包将被丢弃，不进行传送。如果是成员端口，那么，交换机将进一步判定目的端口是否是标记VLAN 的成员端口。如果不是，那么，该数据包也将被丢弃；反之，该数据包将被转发到目的端口。

如果数据包中不包含VLAN 信息（即未被加过标记），那么，入端口将用其PVID 作为数据包的VID 为数据包加上标记（如果该端口是tagging port）。交换机随后判断目的端口是否与入端口属于同一个VLAN（即具有相同的VID），如果不是，那么，该数据包将被丢弃，不进行传送。反之，该数据包将被转发到目的端口。

这就是入站过滤（*ingress filtering*）。在入端口处就丢弃掉那些不在同一个VLAN 中的数据包，可以尽可能地保存带宽， 减少后续的目的端口处理数据包的工作量。

4.9 广播风暴（Broadcast）的管理

广播（Broadcast）是指将数据包发送给局域网内所有连接的设备。广播对任何一个网络来说，都是至关重要的。但是，广播经常在网络中引起问题，有时甚至导致整个网络崩溃。因此，交换机必须提供多种功能用于管理网络中的广播数据包。

4.9.1 广播风暴（Broadcast Storm）

广播风暴（Broadcast storm）是当今网络中常见的问题。通常，当广播数据包在网络中大量

传送，或者在网络中循环传送时，会引起网络性能明显地下降，极限情况时将使网络整体瘫痪。引起广播风暴的原因有：存在着网络环路、故障网卡、不良的线路连接，或者一些产生广播的应用程序或协议等。

广播风暴的问题早就引起了网络管理员的关注，并已经在使用传统的路由器来抑制广播风暴的出现。即使可能会在局部地区发生一些广播风暴，也会竭尽全力将其限制在一定的区域内。但是，借助VLAN 的特点，现在交换机拥有比路由器更好的抑制广播风暴的能力，而且，许多交换机还在每个端口内置了侦测和过滤广播包的功能，以进一步控制广播风暴的发生。

4.9.2 分割广播域（Segmenting Broadcast Domains）

VLAN 可以被用于分割广播域（broadcast domain）。由于交换机在转发数据包时，范围仅限于在属于同一个VLAN 的成员间进行数据包传递，这样，网络的其他部分可以被有效地保护起来，免于频繁地受广播风暴的影响。因此，广播域被分割得越小，广播风暴的影响也就越小。

4.9.3 减少广播风暴（Eliminating Broadcast Storms）

SNMP 代理（SNMP agent）可以监视交换机端口上发生广播风暴的次数，一旦端口上的广播风暴发生的次数超出预先限定的上升阈值（*rising threshold*）时，将会触发一个相应的动作。例如，通常的动作是该端口将被阻塞住，并丢弃所有接收到的从其所连接的网络部分来的广播包。而当广播包的数量又低于设定的下降阈值（*falling threshold*）时，SNMP 代理将解除该端口的阻塞状态，使该端口恢复到正常的工作状态。

在S4408MF 交换机上，100Mbps 快速以太网端口和1000Mbps 千兆以太网端口的缺省的触发阈值为每秒128,000 个广播包（即128Kpps）。触发阈值可以针对不同类型的端口分别设置不同的数值，可以通过SNMP 管理软件或者通过控制台界面方便地进行修改。

4.10 组播（Multicasting）

组播（Multicasting）是指一个源地址可以同时发送数据包给多个目的地址，并且这种连接至少需持续一段时间。组播的主要优点是相对于广播来说可以减少网络上的负载。

4.10.1 组播组（Multicast Group）

IP v4 地址共有三类：单播（unicast）、组播（multicast）和广播（broadcast）。单播地址用于单个网络设备发送信息给单个目的网络设备。广播是指发送数据包给子网（subnetwork）上的所有网络设备。组播地址定义一组能够接收组播数据包的网络设备，这些组播组成员可以不在同一个子网上。组播地址用于发送组播数据包（multicast packet）给组播组内的所有成员（group member）。

4.10.2 组播地址（Multicast Addressing）

D 类IP 地址为组播地址。一个D 类的IP 地址用于指派给一个组播组（multicast group）。D 类IP 地址的前4 个比特的特征位为“1110”，其后的28 个比特的数值被称为“ 组播组ID（multicast group ID）”。其中有一些D 类IP 地址被IANA（ Internet Assigned NumbersAuthority）组织预留，不能使用。从224.0.0.1 开始到224.0.0.255 的组播地址被留作路由协议（routing protocol）和一些其他低级的拓扑发现或维护协议（ low-level topology discovery or maintenance protocol）使用。从239.0.0.0 开始到239.255.255.255 的地址被留作本地管理应用（local site administrative applications）使用，而不是
Internet 应用（Internet-wide applications）使用。还有一些D 类IP 地址被一些知名的组别（ 例如，“all routers on this subnet” ， “allDVMRP routers”）所留用。

4.10.3 IGMP V1和V2

组播的基本动作是加入（joining）和离开（leaving）组播组（multicast group）。IGMP 将提供主机加入或者离开组播组的方法。作为IP 层的一部分，IGMP 具有固定长度的数据包，且没有可选的数据。IGMP 数据包（IGMP packet）的格式如下：

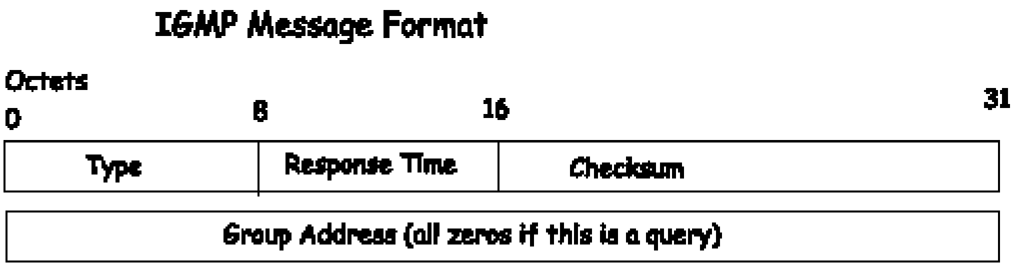


图 4－5 IGMP 消息格式

每个主机（host）都可以加入（join）一个组播组（multicast group）或者离开（leave）一个组播组。规则如下：

- 主机发送一个 IGMP“报告（report）”，申请加入一个组播组。
- 当主机想离开一个组播组时，主机将不再发送报告（report）。——IGMP V1 版
- 当主机想离开一个组播组时，主机将发送一个“离开（leave）”的报告（report）。——IGMP V2 版

组播路由器（Multicast routers）发送IGMP 询问（IGMP queries）(给所有主机的地址：224.0.0.1)。然后，定期查看子网上是否还有组播组成员存在。如果没有来自组播组的回应，那么，路由器将认为网络上不存在组播组成员。

注意：询问消息（query message）中的TTL 字段被设置为1，这样，询问就不会被转发

到其他子网路由器是根据接收到的主机发出的报告（report）来决定是否转发组播数据包给特定的接口（particular interface）的。

IGMP V2 版是IGMP V1 版的加强版，包含一些新的功能，例如为每个LAN 选取组播询问者（multicast querier）、为更快速地删除组播组成员发出明确的离开消息， 以及组询问消息（group-specific querymessage）。具有最小IP 地址的（lowest IP address）路由器将被选为询问者（querier）。明确的组播组离开消息可以降低协议的反应时间（latency），路由器可以以特定的组IP（particular group ID）寻找报告（report）。IGMP V3 版目前处于起草阶段，此版IGMP 使得主机可以加入一个组播组，同时指定欲接收组播消息的源组播组。IGMPV2 版中的离开组播组的消息（leave group message）已经增加了支持组源离开消息（group-source leave message）。

注意：目前的软件版本暂不支持组播，在 S4408MF 下一个软件升级版本中会支持组播协议。

第五章 Console接口配置

S4408MF 交换机提供一个控制台管理界面（console management interface），使你可以通过其对交换机进行设置和控制管理。你可以利用一个终端设备（仿真终端也可以），或者利用TCP/IP的**TELNET**功能，登录到控制台界面，以进行许多最基本的网络管理操作。本章内容就是向您介绍如何通过控制台界面来访问交换机，更改交换机的设置，以及监视交换机的运行状态的。

5.1 概括介绍

1. 确定网络如何将最好的分段。这将在一个已有二层交换机的网络内运用 VLAN 功能。
2. 设计 IP 地址的配置。其包括将 IP 地址分配给每个网段。每个网段被分配网络地址和子网掩码。
3. 确定哪些网络资源必须在网段中共享。共享资源可能直接连接在三层交换机上，如果需要，应该确定静态路由到每个共享资源上。
4. 确定每个子网如何与广域网或 Internet 相连接。另外，静态路由应该确定相应的默认网关。
5. 确定安全设计。一些子网需要更多的安全性或应同其它子网进行隔离。这将使用到 IP 或 MAC 地址过滤. 同样, 一个或更多的 VLAN 在三层交换机上也可以不配置一个 IP 子网－在某些案例中，VLAN 的功能将类似一个二层 VLAN，另外将需要一个外部的路由器来连接整个网络。
6. 策略设计。一些子网将需要大量的组播带宽，策略就是一种机制,如在一个网络设备上改变正常的包转发方式，能够智能的分配带宽给急需的应用如视频、音频和大量数据等。
7. 确定冗余设计。计划冗余连接和网络重要资源路由能在一旦链路或设备出现故障时产生挽救措施。S4408MF 的 SpanningTree 功能可以用于冗余链路连接。

5.2 如何登录控制台界面

通过 Console 口进行管理时，必须用一根 RS-232C 电缆将一台兼容 VT-100 的终端或者一台运行终端仿真程序（如 Windows95/98/2000 操作系统中的超级终端）的 PC 机，连接到 S4408MF 交换机前面板上的“ Console ”接口，然后，在终端上采用如下参数，就可以登录到控制台界面。所需的设置参数如下：

Baud rate:	9,600
Data width:	8 bits
Parity:	none
Stop bits:	1
Flow Control ：	none

典型的和 Console 口的连接方法如下图所示：

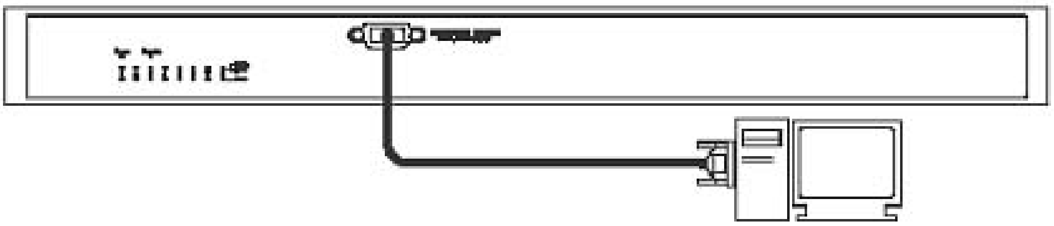


图 5-1 与 Console 口的连接方法举例

在 Windows95/98/2000 下，执行“ 超级终端 ”的“ Hypertrm.exe ”,进行新建连接。在图标一栏中，选择电话图标->在“连接使用中 ”选择“ 直接连接到串口 1 ”或其他串口 -> 按“确认 ”键盘->在“端口设置”中选择波特率为“ 9600 ”、数据位为“ 8 ”、奇偶校验“ 无 ”、停止位为“ 1 ”、流量控制为“ 无 ”。进入“ 超级终端 ”界面后，按“ ENTER ”键，就可以进入控制台界面了。

此外，用户也可以利用 Telnet 来登录控制界面。一旦一个交换机已经被赋予一个 IP 地址后，你就可以利用 Telnet 命令（VT-100 兼容终端）通过网络来访问和控制交换机。实际上，用这两种方式登录到控制台界面后，所看到的和所操作的是一样的。但用户用 Telnet 登录控制台界面有两个前提：

前提一是在交换机的控制管理中必须有超级用户的存在，用户的优先级为 15 的用户为超级用户。第一次登录控制台界面添加用户和设置用户权限时必须依靠 Console 口进行登录。

前提二是必须为该交换机配置一个可行的 IP 地址。

5.2.1 配置超级用户

当用户第一次用 Console 口登录控制台界面时显示如图 5-2 所示：

该设备出厂时缺省用户名称是 **admin**，密码是 **password**。用户敲入相应的用户名和密码后就可以对交换机进行管理控制，既在”switch”的提示符下键入相应命令。

注意：登录交换机的口令是区分大小写的，“ S ” 与 “ s ” 不同。

在这里只给出如何通过 Console 口进行添加用户和设置用户权限，具体操作如图 5-3 所示。

1．用户在 Switch#下敲入”configure”命令。

2．在 Switch(config)#下敲入”user”命令，会显示出两个对用户操作的命令：添加和删除；

3．用户继续敲入”useradd tp”，则添加了一个用户名为”tp”的用户；

4．用户在”password”提示下设置密码，在”enteragain”下确认密码；

5．用户在”accesslevel”的提示下设置用户的权限，用户的权限有两个级别：管理员级别（Adminitrator）(也叫超级用户)和普通用户级别（Normal User）,将权限设置为 15 既表示该用户拥有管理员级别。

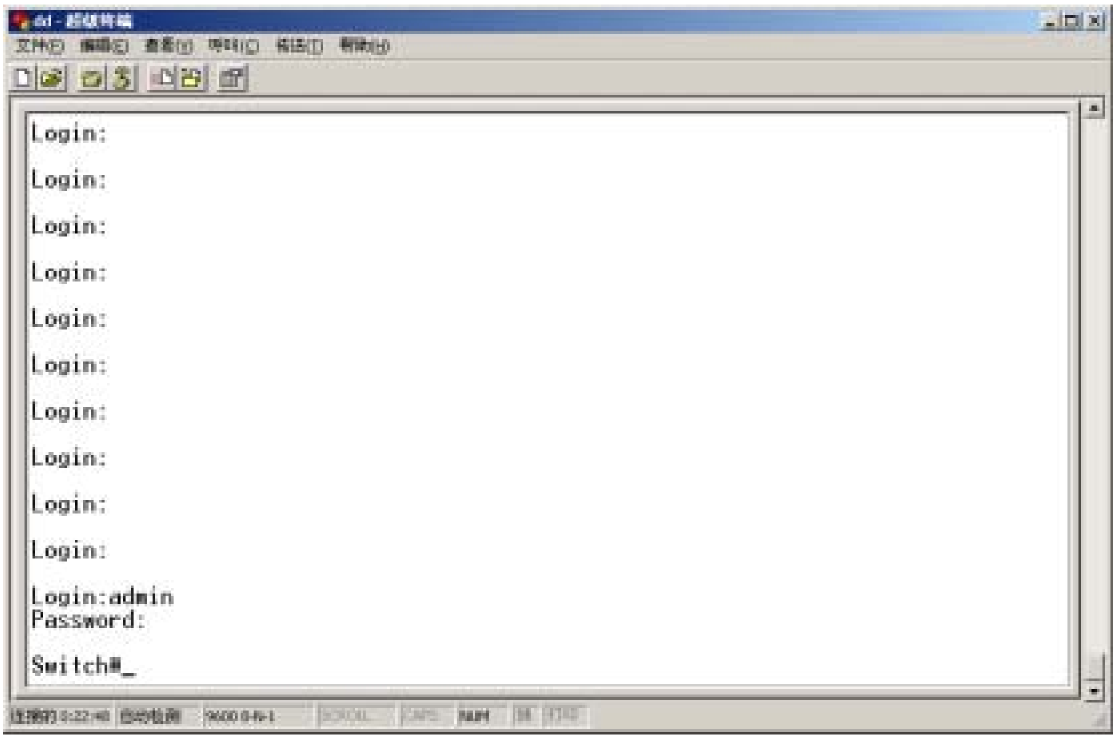


图 5-2 用 CONSOLE 口登录的初始界面

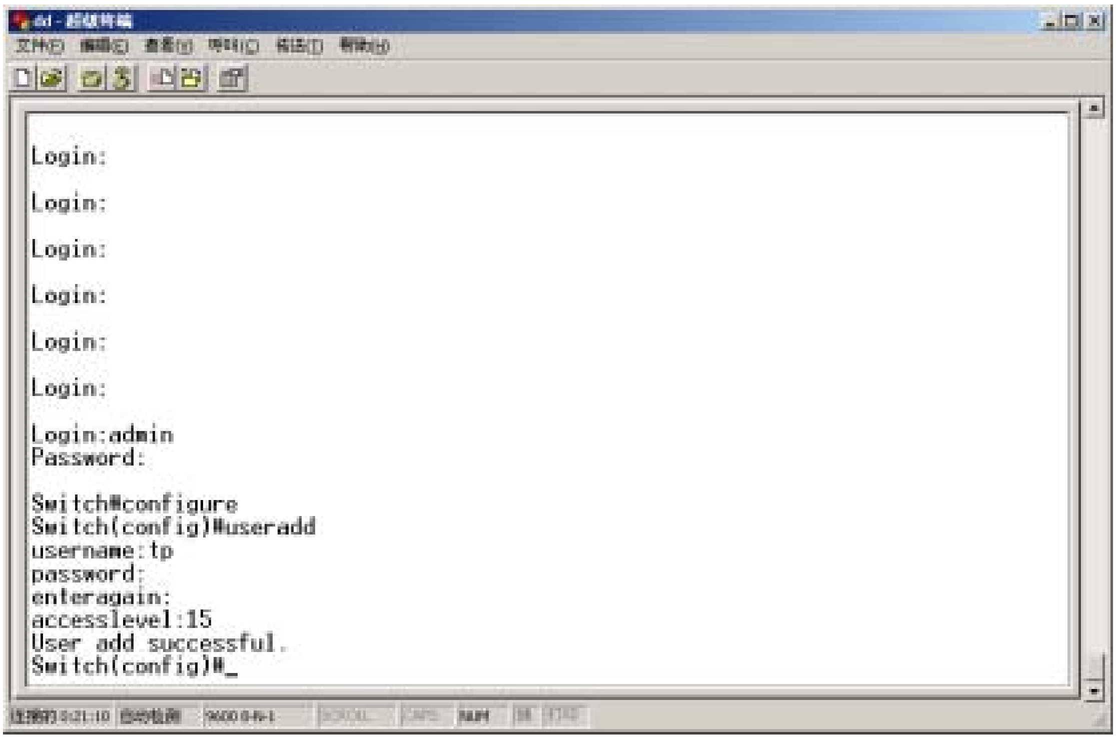


图 5-3 添加用户的界面

管理员级别的权限比普通用户级别的权限高，有一些菜单普通用户级别的用户就不允许访问或更改设置，普通用户也不能通过 Telnet 对控制台界面进行访问和控制。下表是关于普通用户权限和管理员权限的详细说明：

菜单（menu）	管理员级（Administrator）	普通用户级（Normal User）
	权限	
更改配置	Read/Write	Yes, read only.
网络监测	Read/Write	Yes, read only.
一致性字符串和陷阱的设置（Community Strings and Trap Stations）	Read/Write	Yes, read only.
升级固件（Firmware）和配置文件（Configuration Files）	Read/Write	Yes, read only.
帐户管理（User Accounts Management）		
创建/更改帐户	Read/Write	No
查看/删除帐户	Read/Write	No
系统利用	Read/Write	Yes, (Ping Test); 其余的 read only
恢复出厂默认设置	Read/Write	No
重启系统	Read/Write	No

5.2.2 配置交换机IP地址

由于 S4408MF 不提供带外管理接口，在系统启动后必须通过 Console 口为交换机配置一个带内 IP 地址。有了该 IP 地址后，通过 Telnet 登录控制台界面或通过 Web 登录 Web 网络管理界面才能成为可能。

系统启动时配置了缺省的 VLAN 1，用户只需用配置命令设置一个 Supervlan，既为该交换机设定了 IP 地址。

如何配置 Supervlan 在下面章节中会详细介绍，这里只简要说明如何马上使用该命令，因为为交换机配置 IP 地址是第一步。

1．用户在 Switch#下敲入”configure”命令。

2．在 Switch(config)#下敲入 subvlan ？

3．根据提示的帮助信息将 subvlan 和 vid 进行绑定，缺省的 vid 为 1，该命令在配置 subvlan 中有详细说明。

3．在 Switch(config)#下敲入 supevlan ？

4．根据提示的帮助信息依次敲入各项内容，其中"ipaddress"项用来配置 IP 地址，该命令在配置 supervlan 中有详细说明。

具体流程如图 5－4 所示：

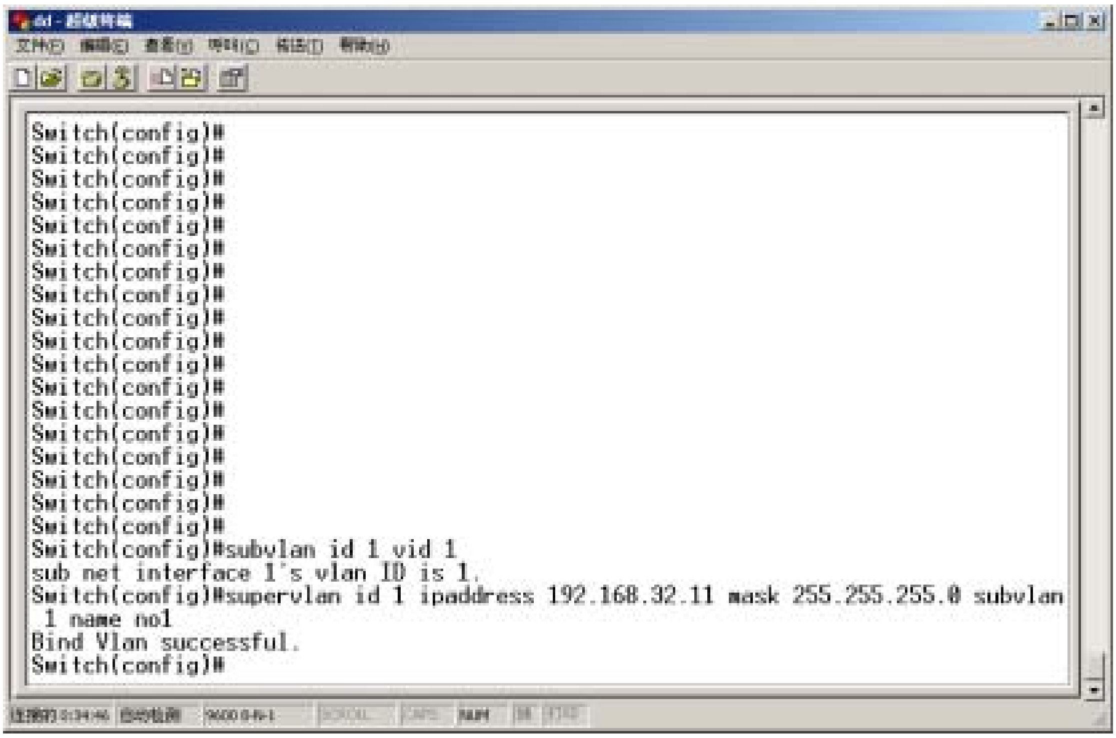


图 5－4 配置 IP 地址的界面

图中 Supervlan 的 IP 地址为 192.168.32.249，子网掩码为 255.255.255.0，subvlan 的 ID 号为 1。下面就以 Telnet 命令登录控制台界面为例，详细介绍如何使用各种 CLI 命令。

5.3 CLI命令使用说明

5.3.1 一些特殊键的使用

console 口支持下列的特殊键：

Tab 键：输入命令的前一部分后，键入 Tab 后可以显示出的整的命令。例如：

键入 sh 后按 Tab 键，则显示出 show 命令。

CTRL-n：向下翻滚命令的历史记录；

CTRL-p：向上翻滚命令的历史记录；

CTRL-b：把光标向左移动一格；

CTRL-f：把光标向右移动一格；

CTRL-d：删除光标上的一个字符；

CTRL-z：推出当前节点，等同于命令 exit；

向上方向键：向上翻滚命令的历史记录；

向下方向键：向下翻滚命令的历史记录；

当一屏幕显示不下时，可以分屏显示。当一屏幕显示不下时，会出现-more- 提示，这时空格键使屏幕向上滚动一屏幕，回车键向上滚动一行。

5.3.2 语法帮助

命令行接口中内置有语法帮助。如果对某个命令的语法不太确定，请输入该命令中已知道的前面的部分，然后键入“？”或“空格加？”。命令行会提示已经输入的部分命令剩余部分的可能的

命令清单。这样就可以根据提示的命令继续输入命令，直至提示命令为<cr> 时，表明命令输入完毕。按回车就可以执行所键入的命令。

【举例】

Switch#set po

在输入“ set po ”之后键入“ ? ”，显示下面的内容：

port

提示完整的命令为 set port 。

如果是加入空格后再键入“ ? ”，会显示下面的提示信息：

<String>   <1-8/all> port list

提示下面的输入参数，在上面的例子中为端口列表或者选择全部的端口。

5.3.3 使用语法帮助补齐命令

系统提供输入“ tab ”键补全命令的功能。也就是用户输入部分命令，然后输入“ tab ”键，系统自动检索匹配的命令如果检索到相应的命令，系统可以自动补齐。如果检索到多个命令，系统会显示可选择的命令。

【举例】

Switch(config)#s

save   snmp-server   spanning-tree   subvlan

supervlan

在上面的例子中，键入“ s ”后，使用“ tab ”键，因为有多个以“ s ”开头的命令，命令行会显示全部以“ s ”开头的命令。

如果在“ s ”后键入“ p ”，再使用“ tab ”键，这时候只检索到 spanning-tree 命令，系统会自动补齐。

Switch(config)#spanning-tree

5.3.4 命令帮助使用说明

在下面所有的命令行帮助信息中，对命令和参数进行了区分，在键入的例子中，用粗体字来表示命令，用一般字体表示参数。

系统对于输入的大小写进行区分，因此对于输入的命令和参数的大小写要严格一致，否则系统会提示错误。

5.3.5 常用命令

5.3.5.1 help命令

用户使用 help 命令显示系统帮助信息。

【使用指南】 S4408MFCLI 配置提供随时随地的在线帮助，用户也可以随时键入“ ？ ”获取在线帮助。

【举例】

Switch#**help**

Help may be requested at any point in a command by entering a question mark '?'.
If nothing matches, the help list will be empty and you must backup until entering a '?'
shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a command argument (e.g. ' show ?') and describes each possible argument.
2. Partial help is provided when an abbreviated argument is enteredand you want
to know what arguments match the input(e.g. 'show pr?'.)

Switch#

5.3.5.2 禁止命令disable

用户执行该命令设置当前用户的优先级为更低的优先级。

【命令格式】disable <0-15>

【使用指南】该命令在根指示符下执行，降低当前用户权限为更低级别。目前情况下，级别 15 是管理员级别，取得该级别权限的用户，可以对交换机进行任何的操作，包括设置和设置信息的显示，以及对于用户的管理。低于 15 而高于 10 的级别可以使用“ rcommand ”命令，其它的设置命令都不可用。低于 10 的级别只能显示基本信息，不能进行任何的设置。如果要对交换机进行设置，需要使用“ enable ＋级别 ”命令来提高自己的级别。具体的使用方法参照下面关于 enable 命令的说明。

【参数说明】<0-15>为优先级编号，范围为 0-15，为可选参数，默认为 0。

【举例】

Switch＃**disable** 0

Switch>

5.3.5.3 允许命令enable

用户执行该命令设置当前用户的优先级为更高优先级。

【命令格式】enable <0-15>

【使用指南】该命令在根指示符下执行，升高当前用户权限为更高级别。如果设置优先级为 15，则可以变为管理员级用户，可以重新登录该 CLI 配置界面。

【参数说明】<0-15>为优先级编号，范围为 0-15，为可选参数，默认为 15。

【举例】

Switch＃**enable** 15

Login：

Password:

Switch＃

5.3.5.4 arp命令

用户执行该命令配置静态 ARP 表。

【命令格式】1. arp ip <A.B.C.D> mac-addr < HH:HH:HH:HH:HH:HH >

2. no arp ip <A.B.C.D>

3. no arp all

【使用指南】命令 1 添加一个 ARP 表项；

命令 2 删除一个 ARP 表项。

命令 3 删除所有的 ARP 表项。

【参数说明】<A.B.C.D>为点分十进制方式的 IP 地址，这个 IP 地址必须和交换机中已经设定的 supervlan 的 ip 地址在同一个网段，否则设置不成功。< HH:HH:HH:HH:HH:HH >表示 MAC 地址。

【举例】

Switch(config)#**arp ip** 192.168.32.100 **mac-addr** 00:20:34:e2:56:f4

Successfully add arp entry.

Switch(config)#

Switch(config)#**no arp ip** 192.168.32.100

Successfully delete arp entry.

Switch(config)#

Switch(config)#**no arp all**

Successfully clear all arp entries.

Switch(config)#

5.3.5.5 clock命令

该命令用于配置系统的时钟，可以使用相应的 show 命令来显示设置的结果和当前设定的日期时间参数。

【命令格式】set clock <yyyy-mm-dd-HH-MM-SS>

【使用指南】<yyyy-mm-dd-HH-MM-SS>的输入要求严格遵守手册或者帮助给定的日期输入格式。在例子中显示的时间的短暂差异为输入命令的时延。

【举例】

Switch#**set clock** 2003-7-9-13-26-9

Successfully set date and time.

Switch#

可以用下面的命令显示设置的结果。

Switch#**show clock**

Current date time is :2003-7-9-13-26-40

Switch#

5.3.5.6 hostname命令

用户使用 hostname 命令配置设备名称。

【命令格式】hostname <name>

【参数说明】<name> 为最大长度为 128 的字符串，用于表示设备名称。

【举例】

Switch<config>#**hostname** test-switch

Host name set to test-switch

test-switch #**show hostname**

Host name is : test-switch

test-switch #

5.3.5.7 保存配置命令save

用户执行该命令保存当前的所有配置。

【命令格式】save

【使用指南】该命令在 configure 配置路径下有效，无参数。

【举例】

Switch<config>#**save**

Save current configure to NVM is processing,Please wait...#################

#########################OK.

Switch<config>#

5.3.5.8 复位命令reset

用户执行该命令用于重新启动设备。

【命令格式】reset

【使用指南】该命令必须在 configure 配置路径下才有效，用于系统热启动。

【举例】

Switch<config>#**reset**

Device resetted. Please connect again.

5.3.5.9 回复配置命令resettodefaults

用户执行执行该命令时，设备重新启动并且恢复到出厂时的配置。

【命令格式】resettodefaults

【使用指南】该命令必须在 configure 配置路径下才有效，用于系统热启动，并恢复出厂设置。

【举例】

Switch<config>#**resettodefaults**

Device reset to default. Please connect again.

5.3.5.10 终端设置

baud rate 命令

该命令用于设置 console 口的波特率。

【命令格式】1. baud rate <2400|9600|19200|38400>

2. no baud

【使用指南】命令 1 设置 console 口波特率,命令 2 恢复 console 波特率的缺省值,缺省值为 38400。

【参数说明】<2400|9600|19200|38400>为要设定的 console 口波特率，取值为 2400，9600，19200，38400。

【举例】

Switch#**configure**

Switch(config)#**terminal**

Switch(con-term)# **baud rate** 9600

Baud rate is set to 9600

Switch(con-term)#

length 命令

该命令用于设置 console 口的输出高度。

【命令格式】1.length <20-40>

2.no length

【使用指南】命令 1 设置 console 口的输出高度，命令 2 恢复 console 输出高度的缺省值，缺省值为 25。

【参数说明】<20-40>为 console 口的高度值，取值范围为 20-40。

【举例】

Switch(con-term)#**length** 20

Terminal length is set to 20

Switch(con-term)#

width 命令

该命令用于设置 console 口的输出宽度。

【命令格式】1.width <60-80>

2.no width

【使用指南】命令 1 设置 console 口的输出宽度，命令 2 恢复 console 输出宽度的缺省值，缺省值为 80。

【参数说明】<60-80>为 console 口的宽度值，取值范围为 60-80。

【举例】

Switch(con-term)# **width** 70

Terminal width is set to 70

Switch(con-term)#

可以用下面的命令显示端口设置的结果

Switch#**show terminal**

Terminal baud rate is 9600

Terminal width is 70

Terminal length is 20

Switch#

5.3.5.11 ping命令

该命令等同于 Dos 下的 ping 命令。

【命令格式】ping <A.B.C.D> [1-65535]

【参数说明】<A.B.C.D>为点分十进制方式表示的目的 IP 地址；[1-65535]为 ping 报文的数目，该参数可选。

【举例】

Switch#**ping** 192.168.32.166 5

Sending 5, 56-byte ICMP Echos to 192.168.32.166, timeout is 5 seconds:

!!!!!

5 packets received.

Switch#

5.3.5.12 ip route命令

用户执行该命令可设置静态的路由，作为一个特殊情况，用户可以用该命令来完成缺省路由的设置。

【命令格式】1. ip route dest <A.B.C.D> mask <A.B.C.D> nexthop <A.B.C.D> attribute [name

<routername>][hardware][gate]

2. no ip route <A.B.C.D>

【参数说明】dest 后面的<A.B.C.D> 为目的网段，mask 后面的<A.B.C.D>为此网段对应的掩码，这两个参数要严格对应，否则可能设置不成功。Nexthop 后面的<A.B.C.D>为 IP 路由表的下一跳地址。<routername>是路由表项的名称。Hardware 和 gate 是可选项，用于确定路由表的类型。命令 2 用于删除一个路由表项。

注意：下一跳的 ip 地址需要和已经设定的 supervlan 处于同一网段。

【举例 1】设置普通的静态路由

Switch(config)#**ip route dest** 202.106.0.0 **mask** 255.255.255.0 **nexthop** 192.168.32.254 **attribute**

Successfully configure ip route table.

Switch(config)#

Switch(config)#**no ip route** 202.106.0.0

Successfully delete ip route table.

Switch(config)#

可以用下面的命令显示设置的结果

Switch#**show ip route**

```
**************************************************************************
*HW/SW -> HW:hardware SW:software un:unkown                              *
*If(interface) -> 427 system interface                                   *
*Type -> un:unkown iv:invalid dir:direct indir:indirect                  *
*learn-> un:unkown net:netmgmt                                           *
*Dyn(dynamic) -> y:yes n:no                                              *
**************************************************************************
RouteEntry          NextHop           Metric HW/SW   If   Type   Learn Dyn Age(s)
```

127.0.0.1/32	127.0.0.1	0	SW	427	dir	local	y	292
192.168.32.0/24	192.168.32.13	0	SW	427	dir	local	y	293
192.168.33.0/24	192.168.33.111	0	SW	1	dir	local	y	281
192.168.33.254/32	192.168.33.111	0	SW	1	dir	un	y	41
202.106.0.0/24	192.168.33.254	1	SW	1	indir	un	n	41

Switch#

【举例 2】设置缺省路由

Switch(config)#**ip route dest** 0.0.0.0 **mask** 0.0.0.0 **nexthop** 192.168.35.11 **attribute ?**

name The ip route table entry name

hardware Configure the route entry to hardware

gate Configure the route entry as gateway

<cr>

Switch(config)#**ip route dest** 0.0.0.0 **mask** 0.0.0.0 **nexthop** 192.168.32.11 **attribute name** gg **hardware gate ?**

<cr>

Switch(config)#**ip route dest** 0.0.0.0 **mask** 0.0.0.0 **nexthop** 192.168.35.11 **attribute name** gg **hardware gate**

Successfully configure ip route table.

Switch(config)#

在上面的 show 命令输出的信息里，RouteEntry 为 0.0.0.0/0 的路由表项为默认路由表项的设置。

5.3.5.13 配置tftp server

用户在当前配置的提示符下键入“ **tftp ip**”，该命令用于配置 tftp server 的 IP 地址。

【命令格式】tftp ip <A.B.C.D>

【使用指南】tftp server 用于上传下载文件。

【参数说明】<A.B.C.D>为 tftp server 的 IP 地址，以点分十进制表示。

【举例】

Switch(config)#**tftp ip** 10.1.1.8

Successfully set TFTP address.

Switch(config)#

5.3.5.14 download命令

用户执行该命令进行软件的下载。

【命令格式】 download filename <filename> <filetype>

【使用指南】下载（更新）软件前，需要使用命令 **tftp** 配置 tftp server 的位置。

【参数说明】 <filename>为要下载的文件名称，<filetype>为要下载的文件类型（这里支持 application，configuration 两种类型文件）

【举例】

Switch<config>#**download filename** switch.z application

Download file.Please wait################################OK.

注意：要使用该命令，必须先配置交换机的一个 ip 地址。

如果源主机配置了防火墙，执行 download 命令操作失败。

5.3.5.15 upload命令

用户执行该命令 upload 设备上运行的软件。

【命令格式】upload configfile <filename >

【使用指南】下载（更新）软件前，需要使用命令 **tftp** 配置 tftp server 的位置。

【参数说明】<filename >为上传软件后软件的名称和位置（字符串形式）；

【举例】

Switch<config>#**upload configfile** “c:\switch\vxworks.z”

Switch<config>#

注意：要使用该命令，必须先配置交换机的一个 ip 地址。

如果目的主机设置了防火墙，使用该命令会操作失败。

5.3.5.16 退出命令exit 、Ctrl+z

从当前的节点退回到上一节点，如果当前是根结点，则退出当前会话。

【命令格式】exit

【举例】

Switch(config-if)#**exit**

Switch(config)#**exit**

Switch#

【命令格式】Ctrl+z

【使用指南】此命令直接从当前节点退到根节点

【举例】

Switch(config-if)#

Switch#

5.3.6 用户管理命令

5.3.6.1 添加用户命令

用户执行该命令进行添加用户操作。

【命令格式】useradd <username>

【使用指南】用户输入“ useradd ”后，会执行“ 输入密码 ”、“ 确认新密码 ”、“ 访问级别 ”三步操作。为安全起见，这里输入的字符串都不回显。访问级别为 15 的是超级用户（管理员级别）。

【参数说明】<username>为用户名称，以字符串表达，可以输入的是 26 个英文字符的大小写或者数字的组合，不可以是其它字符或者不可显示的字符；访问级别的取值范围是 0－15。15 是最高级别。

【举例】

Switch<config>#**useradd** “user”
password:
enteragain:
accesslevel:15
User add successful
Switch<config>#

可以用下面的命令显示设置的结果。

Switch#**show user**

User name	Password	Access level	Property
user	user	15	0

Switch#

5.3.6.2 删除用户命令

用户执行该命令进行删除用户操作。

【命令格式】userdelete <username>

【参数说明】<username>为用户名称，以“ ”字符串表达。

【举例】

Switch<config>#**userdelete** “user”

User delete successful

Switch<config>#

5.3.6.3 配置密码

用户执行该命令用于修改用户登录密码。

【命令格式】password

【使用指南】用户输入“ password ”后，会执行“ 输入旧密码 ”、“ 输入新密码 ”、“ 确认新密码 ”三步操作。为安全起见，这里输入都不回显。

【举例】

Switch<config>#**password**

oldpassword:

newpassword:

enteragain:

Password change successful.

Switch<config>#

5.3.7 配置交换机端口命令

用户执行下述命令进行交换机物理端口的配置项。

【命令格式】set port <portlist |all> +设置项

【使用指南】使用端口设置命令可以对交换机物理端口的一些属性进行设置，在上面的命令中包括了多个可能的设置项。

【参数说明】参数为交换机物理端口列表，输入的形式可以是“1－2”或者“1，2，4－6”，如果要设置全部的物理端口可以使用“all”参数项。

【举例】

Switch#**set port** ？

<String> <1-8/all> port list

5.3.7.1 端口禁用命令

用户执行该命令关闭指定的端口。

【命令格式】set port <portlist |all> disable

【使用指南】<portlist |all>为交换机物理端口列表，输入的形式可以是“1－2”或者“1，2，4－6”，如果要设置全部的物理端口可以使用“all”参数项。

【举例】

Switch#**set port** all **disable**

Successfully shutdown ports.

Switch#

5.3.7.2 端口使能命令

用户执行该命令使能指定的端口。

【命令格式】set port <portlist |all> enable

【使用指南】<portlist |all>为交换机物理端口列表，输入的形式可以是“1－2”或者“1，2，4－6”，如果要设置全部的物理端口可以使用“all”参数项。

【举例】

Switch#**set port** all **enable**
Successfully enable ports.
Switch#

5.3.7.3 端口风暴控制命令

该命令集用于配置端口风暴控制。

广播风暴控制命令

该命令设置指定的端口是否允许广播报文流过。

使能广播风暴控制

【命令格式】set port <portlist |all> storm-weaken broadcast enable

【参数说明】<portlist |all>为交换机物理端口列表，输入的形式可以是“1－2”或者“1，2，4－6”，如果要设置全部的物理端口可以使用“all”参数项。

【使用指南】当设置的物理端口号在 1－8 之间取任意值时，1－8 端口都将被设置

【举例】

Switch#**set port** 5-8 **storm-weaken broadcast enable**
Successfully enable ports' broadcast.
Switch#

使用 show port storm-weaken 命令可以看到设置的结果。

Switch#**show port storm-weaken**

Port	Pause Flood	Broadcast	Multicast	Rate
1	disable disable	enable	disable	1000
2	disable disable	enable	disable	1000
3	disable disable	enable	disable	1000
4	disable disable	enable	disable	1000
5	disable disable	enable	disable	1000
6	disable disable	enable	disable	1000
7	disable disable	enable	disable	1000
8	disable disable	enable	disable	1000

Switch#

禁止广播风暴控制命令

【命令格式】set port <portlist |all> storm-weaken broadcast disable

【参数说明】<portlist |all>为交换机物理端口列表，输入的形式可以是“1－2”或者“1，2，4－6”，如果要设置全部的物理端口可以使用“all”参数项。

【使用指南】当设置的物理端口号在 1－8 之间取任意值时，1－8 端口都将被设置

【举例】

Switch#**set port** 5-8 **storm-weaken broadcast disable**

Successfully forbidden ports' broadcast.

Switch#

使用 show port storm-weaken 命令可以看到设置的结果。

Switch#**show port storm-weaken**

Port	Pause	Flood	Broadcast	Multicast	Rate
1	disable	disable	disable	disable	1000
2	disable	disable	disable	disable	1000
3	disable	disable	disable	disable	1000
4	disable	disable	disable	disable	1000
5	disable	disable	disable	disable	1000
6	disable	disable	disable	disable	1000
7	disable	disable	disable	disable	1000
8	disable	disable	disable	disable	1000

Switch#

洪泛报文控制命令

该命令设置指定的端口是否允许洪泛报文流过。

使能洪泛报文控制命令

【命令格式】set port <portlist |all> storm-weaken flood enable

【参数说明】<portlist |all>为交换机物理端口列表，输入的形式可以是“1－2”或者“1，2，4－6”，如果要设置全部的物理端口可以使用“all”参数项。

【使用指南】当设置的物理端口号在1－8之间取任意值时，1－8端口都将被设置

【举例】

Switch#**set port** 7-8 **storm-weaken flood enable**
Successfully enable ports' flood.
Switch#

使用 show port storm-weaken 命令可以看到设置的结果。

Switch#**show port storm-weaken**

Port	Pause	Flood	Broadcast	Multicast	Rate
1	disable	enable	disable	disable	1000
2	disable	enable	disable	disable	1000
3	disable	enable	disable	disable	1000
4	disable	enable	disable	disable	1000
5	disable	enable	disable	disable	1000
6	disable	disable	disable	disable	1000
7	disable	enable	disable	disable	1000
8	disable	enable	disable	disable	1000

Switch#

禁止洪泛报文控制命令

【命令格式】set port <portlist |all> storm-weaken flood disable

【参数说明】<portlist |all>为交换机物理端口列表，输入的形式可以是"1－2"或者"1，2，4－6"，如果要设置全部的物理端口可以使用"all"参数项。

【使用指南】当设置的物理端口号在 1－8 之间取任意值时，1－8 端口都将被设置

【举例】

Switch#**set port** 7-8 **storm-weaken flood disable**

Successfully forbidden ports' flood.

Switch#

使用 show port storm-weaken 命令可以看到设置的结果。

Switch#**show port storm-weaken**

Port	Pause	Flood	Broadcast	Multicast	Rate
1	disable	disable	disable	disable	1000
2	disable	disable	disable	disable	1000
3	disable	disable	disable	disable	1000
4	disable	disable	disable	disable	1000
5	disable	disable	disable	disable	1000
6	disable	disable	disable	disable	1000
7	disable	disable	disable	disable	1000
8	disable	disable	disable	disable	1000

Switch#

组播报文控制命令

该命令设置指定的端口是否允许组播报文流过。

允许组播报文通过命令

【命令格式】set port <portlist |all> storm-weaken multicast enable

【参数说明】<portlist |all>为交换机物理端口列表，输入的形式可以是“ 1－2 ”或者“ 1，2，4－6 ”，如果要设置全部的物理端口可以使用“ all ”参数项。

【使用指南】当设置的物理端口号在 1－8 之间取任意值时，1－8 端口都将被设置

【举例】

Switch#**set port** 7-8 **storm-weaken multicast enable**

Successfully enable ports' multicast.

Switch#

使用 show port storm-weaken 命令可以看到设置的结果。

Switch#**show port storm-weaken**

Port	Pause	Flood	Broadcast	Multicast	Rate
1	disable	disable	disable	enable	1000
2	disable	disable	disable	enable	1000
3	disable	disable	disable	enable	1000
4	disable	disable	disable	enable	1000
5	disable	disable	disable	enable	1000
6	disable	disable	disable	enable	1000
7	disable	disable	disable	enable	1000
8	disable	disable	disable	enable	1000

Switch#

禁止组播报文通过命令

【命令格式】set port <portlist |all> storm-weaken multicast disable

【参数说明】<portlist |all>为交换机物理端口列表，输入的形式可以是“1－2”或者“1，2，4－6”，如果要设置全部的物理端口可以使用“all”参数项。

【使用指南】当设置的物理端口号在 1－8 之间取任意值时，1－8 端口都将被设置

【举例】

Switch#**set port** 7-8 **storm-weaken multicast disable**

Successfully forbidden ports' multicast.

Switch#

使用 show port storm-weaken 命令可以看到设置的结果。

Switch#**show port storm-weaken**

Port	Pause	Flood	Broadcast	Multicast	Rate
1	disable	disable	disable	disable	1000
2	disable	disable	disable	disable	1000
3	disable	disable	disable	disable	1000
4	disable	disable	disable	disable	1000
5	disable	disable	disable	disable	1000
6	disable	disable	disable	disable	1000
7	disable	disable	disable	disable	1000
8	disable	disable	disable	disable	1000

Switch#

pause 帧收发命令

该命令设置指定的端口是否能收发 pause 帧。

允许收发 pause 帧命令

【命令格式】set port <portlist |all> storm-weaken pause enable

【参数说明】<portlist |all>为交换机物理端口列表，输入的形式可以是“ 1－2 ”或者“ 1，2，4－6 ”，如果要设置全部的物理端口可以使用“ all ”参数项。

【举例】

Switch#**set port** 7-8 **storm-weaken pause enable**

Successfully enable ports' pause.

Switch#

使用 show port storm-weaken 命令可以看到设置的结果。

Switch#**show port storm-weaken**

Port	Pause	Flood	Broadcast	Multicast	Rate
1	disable	disable	disable	disable	1000
2	disable	disable	disable	disable	1000
3	disable	disable	disable	disable	1000
4	disable	disable	disable	disable	1000
5	disable	disable	disable	disable	1000
6	disable	disable	disable	disable	1000
7	enable	disable	disable	disable	1000
8	enable	disable	disable	disable	1000

Switch#

禁止 pause 帧收发命令

【命令格式】set port <portlist |all> storm-weaken pause disable

【参数说明】<portlist |all>为交换机物理端口列表，输入的形式可以是“1－2”或者“1，2，4－6”，如果要设置全部的物理端口可以使用“all”参数项。

【举例】

Switch#**set port** 7-8 **storm-weaken pause disable**

Successfully forbidden ports' pause.

Switch#

使用 show port storm-weaken 命令可以看到设置的结果。

Switch#**show port storm-weaken**

Port Pause Flood Broadcast Multicast Rate

1	disable disable disable	disable	1000
2	disable disable disable	disable	1000
3	disable disable disable	disable	1000
4	disable disable disable	disable	1000
5	disable disable disable	disable	1000
6	disable disable disable	disable	1000
7	disable disable disable	disable	1000
8	disable disable disable	disable	1000

Switch#

端口流量设置命令

该命令设置指定的端口的流量控制。

【命令格式】set port <portlist |all> storm-weaken flow rate <1-65535>

【参数说明】<portlist |all>为交换机物理端口列表，输入的形式可以是“1－2”或者“1，2，4－6”，如果要设置全部的物理端口可以使用“all”参数项。<1-65535>是可以设置的端口流量，参数的范围是一个大于 1 的长整型值。

【使用指南】当设置的物理端口号在 1－8 之间取任意值时，1－8 端口都将被设置

【举例】

Switch#**set port** 7-8 **storm-weaken flow rate** 100

Successfully set ports' rate.

Switch#

使用 show port storm-weaken 命令可以看到设置的结果。

Switch#**show port storm-weaken**

Port	Pause	Flood	Broadcast	Multicast	Rate
1	disable	disable	disable	disable	100
2	disable	disable	disable	disable	100
3	disable	disable	disable	disable	100
4	disable	disable	disable	disable	100
5	disable	disable	disable	disable	100
6	disable	disable	disable	disable	100
7	disable	disable	disable	disable	100
8	disable	disable	disable	disable	100

Switch#

5.3.7.4 设置端口镜像命令

该命令集用于配置端口的镜像功能。系统支持多端口到一个端口的镜像，并可以分别设置镜像端口的发包和收包。

设定端口镜像状态命令

该命令用于设置指定端口镜像的使能或禁止。

【命令格式】set mirror status <disable|l2|l3>

【参数说明】<disable|l2|l3>为可以设置的端口镜像功能的状态。

【举例】

Switch#**set mirror status** disable

Successfully set mirror mode.

Switch#

设置端口镜像模式命令

该命令用于设置指定端口的镜像模式。

【命令格式】set mirror port <1-8> mode <none|egress|ingress|all>

【参数说明】<1-8>为物理端口号，在 1-8 之间取值；<none|egress|ingress|all>为可以选择的镜像模式。

【举例】

Switch#**set mirror port** 2 **mode** ingress

Port(s) 2 mirror mode set to ingress.

Switch#

选定监听端口命令

该命令用于设置端口镜像的监听端口，从该端口可以捕获被监听端口的报文。

【命令格式】set mirror monitor <1-8>

【参数说明】<1-8>为物理端口号，在 1-8 之间取值。

【举例】

Switch#**set mirror monitor** 2

Port mirror to port 2.

Switch#

注意：使用该命令的前提是已经使用上面的 port 命令设置了镜像端口和镜像模式。

显示端口镜像结果

可以使用 show port mirror 命令显示设置端口镜像的结果。

Switch#**show port mirror**

Port	Mode	Destination
1	none	NULL
2	egress	2
3	none	NULL
4	none	NULL
5	none	NULL
6	none	NULL
7	none	NULL
8	none	NULL

Switch#

5.3.8 虚拟局域网（VLAN）配置命令

5.3.8.1 配置VLAN

在根提示符下键“ vlan ”，进入 vlan 配置节点，对 vlan 数据库进行配置。

【命令格式】vlan

【举例】

Switch#**vlan**

Switch(vlan)#

创建 VLAN 命令

该命令用于添加一个虚拟的 VLAN。

【命令格式】create <1-4094> attribute [name <vlanname>] [eport <portlist>] [fport <portlist>] [uport <portlist>]

【使用指南】命令用于添加新的 VLAN。 [ ]内的配置项是可选的。

【参数说明】<1-4094>为标识一个 vlan 的标识符 VID，该参数是必须的；<vlanname>是所配置 vlan 的名称，为一字符串，最好用“ ”括起来；[eport <portlist>]为允许出端口的范围，用“ xx-xx ”格式表示，“ xx ”表示端口号,也可以是一个单一的端口号；[fport <portlist>]为禁止出端口的范围，用“ xx-xx ”格式表示，“ xx ”表示端口号，也可以是一个单一的端口号；[uport <portlist>]为不带 tag 的端口范围，用“ xx-xx ”格式表示，“ xx ”表示端口号，也可以是一个单一的端口号。

【举例】

Switch(vlan)#**create** 2 **attribute name** vlan2 **eport** 1-4 **uport** 1-4
Successfully create vlan.
Switch(vlan)#

忽略 VLAN 设置并退出命令

该命令放弃当前的 vlan 配置并且退出,和 exit 命令不同的是该命令不保存配置而未启用的 vlan 内容。

【命令格式】abort

【参数说明】无任何参数

【举例】

Switch(vlan)#**abort**

Switch#

应用 VLAN 设置命令

该命令把当前的 vlan 配置生效。

【命令格式】apply

【参数说明】无任何参数

【举例】

Switch(vlan)#**apply**
Successfully apply vlan entries.
Switch(vlan)#

删除 VLAN 设置命令

该命令删除已经配置且正在工作的 vlan。删除没有生效的 vlan 系统会提示删除失败。

【命令格式】delete <1-4094>

【参数说明】<1-4094>为 vlan id。

【举例】

Switch(vlan)#**delete 2**
VLAN 2 was deleted.
Switch(vlan)#

应用 VLAN 设置并退出命令

该命令退出当前的 vlan 配置节点，并且使配置生效。

【命令格式】exit

【参数说明】无任何参数

【举例】

Switch(vlan)#**exit**

Switch#

清空 VLAN 设置命令

该命令用于清空已设置但未生效 vlan 配置。

【命令格式】reset

【参数说明】无任何参数

【举例】

Switch(vlan)#**reset**

Switch(vlan)#

5.3.8.2 配置supervlan

随着网络的发展，网络不断膨胀，网络地址资源日趋紧张。由于 B 类地址的匮乏，现在有许多网络不得不用更多的 C 类地址来代替单个的 B 类地址。这虽然解决了一定的问题，但每个子网不得不维护一个路由表，因此造成了资源的更大浪费。人们提出了超网的概念。可以把几个高位地址相同的子网共用同一个路由表，形成超网。我们的系统中形成超级虚拟网(SuperVLAN)。

➢ 超级虚拟网(SuperVLAN)的好处

超级虚拟网(SuperVLAN)可以带来的好处是帮助供应商提高 IP 地址的利用率，通过聚合可以使所有的在同一子网上的客户（终端用户）通过统一的路由去使用不同的广播域。

给超级虚拟网分配一个子网地址，指定超级虚拟网的路由地址，其他剩余的地址可以分配给

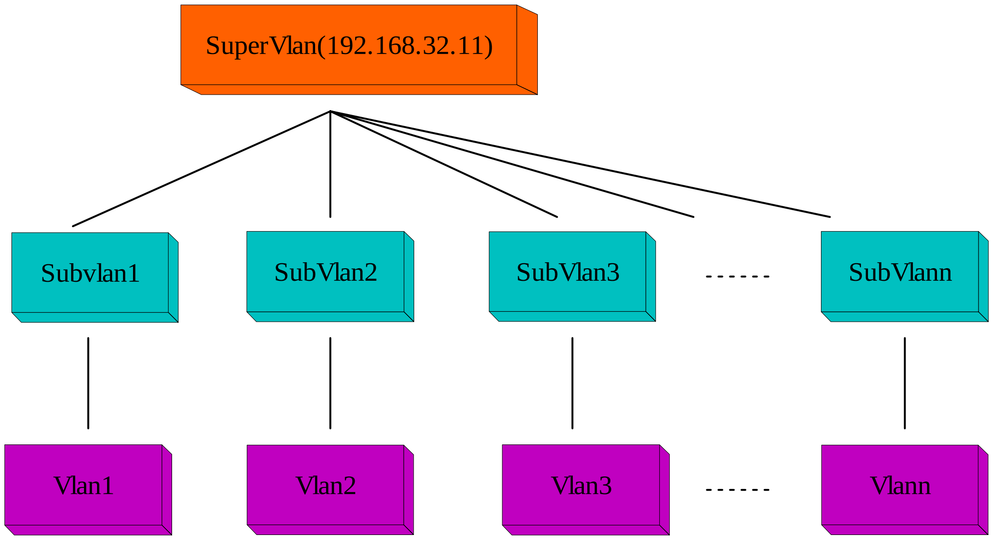
各个主机使用。好像他们只是在同一个大的子网。然后把这个大的子网任意分成若干个“ 子网 ”。这些主机的子网掩码完全相同。超级虚拟网下面只包含子网,不能指定主机。由于各个子网（sub_VLAN）不需要真正的子网网段，有效地提高了 IP 的利用率。这样的子网可以分配足够小，而且可以方便扩展，无需重新定义子网的大小。出于安全目的，可以阻止子网间的相互直接访问，要相互通信需通过路由（因为所有子网的路由都是超级虚拟网的路由地址）。

如果不使用超级虚拟网，每个子网需要设置一个路由地址，而且要分配一个子网地址，结果必然有很多地址被空闲。比如说网络的总容量只需要 3 个 C 类地址的子网，可能不得不申请使用一个 B 类的地址，而 B 类地址数量又很少，因此会造成地址空间的紧张，浪费资源。

➢ 超级虚拟网**(**SuperVLAN**)**的特点

在子网内部的广播，相互通信，不会被发送到子网以外，有效的提供了安全要求。而且子网之间是完全隔离的。所有主机位于同一子网中，他们使用同超级虚拟网一样的子网掩码。使用超级虚拟网地址作为路由地址，可以分配超级虚拟网所在子网的地址有效。所有子网间通信都需要超网路由，不会使用 ARP 的重定向功能直接访问。

下图是关于 supervlan,subvlan,vlan 的关系的示意图。在创建了 vlan 以后，可以通过创建 supervlan 来管理多个 vlan。



SuperVlan,SubVlan,Vlan关系示意图

配置 subvlan 命令

该命令用于绑定 subvlan 和相应的 vlan id。对于一个和 vlan id 绑定的 vlan，可以使用 no subvlan 命令取消绑定的结果。

【命令格式】1. subvlan id <1-16> vid <1-4094>

2. no subvlan id <1-16>

【使用指南】每个有效的 subvlan 都用一个 VID 来标识，命令 2 取消 subvlan 和 vlan id 的绑定，参数为 subvlan 的 ID 号。

【参数说明】<1-16>为 subvlan 编号；<1-4094>为 Vlan ID。

注意：

1．配置 subvlan 的前提是已经配置成功 vlan。

2．如果要删除已经设置的 subvlan，请先取消 supervlan 的设置。

【举例】

Switch<config>#**subvlan id** 1 **vid** 1

Sub net interface 1's vlan ID is 1

Switch<config>#**no subvlan id** 1

Sub net interface 1 has been released

Switch<config>#

配置 supervlan 命令

该命令用于 supervlan 和 IP 地址的绑定。通过设置的 supervlan 的 ip 地址，可以对 supervlan 内的 vlan 进行访问和控制。

【命令格式】 1. supervlan id <1-16> ip <A.B.C.D> mask<A.B.C.D> subvlan <vlanlist> name[supervlanname]

2. no supervlan id <1-16> ip <A.B.C.D>

【使用指南】supervlan 对应的是网络接口，每个 supervlan 由 IP 地址和子网掩码来决定，由 supervlan id 来标识。一个 supervlan 可以包含多个 subvlan。命令 2 用于删除创建的 supervlan，参数为 ID 值和 IP 地址。

【参数说明】<1-16>为 supervlan 的 ID 编号,支持 16 个；ip <A.B.C.D>为 supervlan 的 ip 地址,以点分十进制表示；mask 后面的<A.B.C.D>为 supervlan ip 地址对应的子网掩码，以点分十进制表示；<vlanlist>为 supervlan 聚合的的 subvlan，可以以 1-2,3 的形式设置；[supervlanname]

为 supervlan 名称，为一字符串，最好用“ ”括起来。

注意：

1. **置 supervlan 的前提是 subvlan 已经配置成功。**
2. **同一台设备，可以设置多个 supervlan，但是要保证不同的 supervlan 分配的 ip 地址处于不同的网段，否则，设置不成功。**

【举例】

Switch<config>#**supervlan id** 1 **ip** 10.1.1.1 **mask** 255.0.0.0 **subvlan** 1-2 **name** “example”

Successfully bound vlan.

Switch<config>#**no supervlan id** 1 **ip** 10.1.1.1

The vlan bind has been released.

Switch<config>#

5.3.8.3 设置VLAN端口优先级命令

使用该命令改变端口在 vlan 中的优先级。

【命令格式】set port <portlist|all> priority <0-7>

【参数说明】<portlist|all>为交换机物理端口列表，输入的形式可以是“1－2”或者“1，2，4－6”，如果要设置全部的物理端口可以使用“ all ”参数项；<0-7>为优先级的取值。

【举例】

Switch#**set port** 1-5 **priority** 3

Successfully set 802.1p priority.

Switch#

可以使用 show port priority 命令来显示设置的结果。

Switch#show port priority

port	priority
1	3
2	3
3	3
4	3
5	3
6	0
7	0
8	0

Switch#

5.3.9 生成树协议STP配置命令

生成树协议分为两部分来进行设置，包括基于主机的生成树协议设置和基于端口的生成树设置。

5.3.9.1 基于端口的生成树配置命令

用户执行该命令设置指定端口的 STP 属性。

使能基于端口的生成树协议命令

【命令格式】set port <portlist|all> spanning-tree enable
【使用指南】该命令用于使能基于端口的生成树协议。参数为交换机物理端口列表，输入的形式可以是“1－2”或者“1，2，4－6”，如果要设置全部的物理端口可以使用“all”参数项。

【举例】

Switch#**set port** 1-8 **spanning-tree enable**

Successfully enable ports' stp protocol.

Switch#

禁止基于端口的生成树协议命令

【命令格式】set port <portlist|all> spanning-tree disable

【使用指南】该命令用于禁止基于端口的生成树协议。参数为交换机物理端口列表，输入的形式可以是“1－2”或者“1，2，4－6”，如果要设置全部的物理端口可以使用“all”参数项。

【举例】

Switch#**set port** 1-8 **spanning-tree disable**

Successfully forbidden ports' stp protocol.

Switch#

设定端口路径花销命令

用户执行该命令设置该端口 STP 的端口路径开销。

【命令格式】1. set port <portlist|all> spanning-tree cost <1-65535>

2. no set port <portlist|all> spanning-tree cost

【使用指南】命令 1 设置端口 STP 的端口路径开销，命令 2 恢复它的缺省值。默认情况下，每个 1000Mbps 网段有一个指定的路径开销值为 4

【参数说明】<portlist|all>为交换机物理端口列表，输入的形式可以是“1－2”或者“1，2，4－6”，如果要设置全部的物理端口可以使用“all”参数项。<1-65535>表示端口路径开销的数值。

【举例】

Switch#**set port** 1-8 **spanning-tree cost** 100

Successfully set ports' stp cost.

Switch#

可以用 show spanning-tree interface 命令显示设置的结果。

Switch#**show spanning-tree ethernet**

Designated root priority:8, address:80:00:00:0c:fe:00

Ethernet 1 is Forwarding.

Port path cost 100,Port priority 128.

Designated bridge priority:8,address:80:00:00:0c:fe:00.

Designated port:1,path cost:0.

Ethernet 2 is Forwarding.

Port path cost 100,Port priority 128.

Designated bridge priority:8,address:80:00:00:0c:fe:00.

Designated port:2,path cost:0.

Ethernet 3 is Forwarding.

Port path cost 100,Port priority 128.

Designated bridge priority:8,address:80:00:00:0c:fe:00.

Designated port:3,path cost:0.

Ethernet 4 is Forwarding.

Port path cost 100,Port priority 128.

Designated bridge priority:8,address:80:00:00:0c:fe:00.

Designated port:4,path cost:0.

Ethernet 5 is Forwarding.

Port path cost 100,Port priority 128.

Designated bridge priority:8,address:80:00:00:0c:fe:00.

Designated port:5,path cost:0.

Ethernet 6 is Forwarding.

Port path cost 100,Port priority 128.

-- More --

可以用下面的命令取消设置的结果。

Switch#**no set port** 1-8 **spanning-tree cost**

Successfullly set port path cost to default.

Switch#

下面是取消后显示的结果：

Switch#**show spanning-tree ethernet**

Designated root priority:8, address:82:35:00:40:47:00

Ethernet port 1's stp is disable.

Port path cost 10,Port priority 128.

Designated port is 0,path cost:0.

Ethernet port 2's stp is disable.

Port path cost 10,Port priority 128.

Designated port is 0,path cost:0.

Ethernet port 3's stp is disable.

Port path cost 10,Port priority 128.

Designated port is 0,path cost:0.

Ethernet port 4's stp is disable.

Port path cost 10,Port priority 128.

Designated port is 0,path cost:0.

Ethernet port 5's stp is disable.

Port path cost 10,Port priority 128.

Designated port is 0,path cost:0.

Ethernet port 6's stp is disable.

Port path cost 10,Port priority 128.

Designated port is 0,path cost:0.

Ethernet port 7's stp is disable.

Port path cost 10,Port priority 128.

Designated port is 0,path cost:0.

Ethernet port 8's stp is disable.

-- More --

设定端口 STP 优先级命令

用户执行该命令设置指定端口的 STP 优先级。

【命令格式】1. set port <portlist|all> spanning-tree port-priority <0-255>

2. no set port <portlist|all> spanning-tree port-priority

【使用指南】命令 2 恢复它的缺省值。端口优先权可设置为从 0 到 255 中的一个数值。较小的数值表示端口有较大的可能性被选作为根端口。

【参数说明】<portlist|all>为交换机物理端口列表，输入的形式可以是"1－2"或者"1，2，4－6"，如果要设置全部的物理端口可以使用"all"参数项。<0-255>表示端口生成树优先级数值大小。

【举例】

Switch#**set port** 1-3 **spanning-tree port-priority** 10

Successfully set ports' stp priority.

Switch#

可以使用 show spanning-tree interface 命令显示设置的结果。

Switch#**show spanning-tree ethernet**

Designated root priority:8, address:80:00:00:0c:fe:00

Ethernet 1 is Forwarding.

Port path cost 4,Port priority 10.

Designated bridge priority:8,address:80:00:00:0c:fe:00.

Designated port:1,path cost:0.

Ethernet 2 is Forwarding.

Port path cost 4,Port priority 10.

Designated bridge priority:8,address:80:00:00:0c:fe:00.

Designated port:1,path cost:0.

Ethernet 3 is Forwarding.

Port path cost 4,Port priority 10.

Designated bridge priority:8,address:80:00:00:0c:fe:00.

Designated port:1,path cost:0.

Ethernet 4 is Forwarding.

Port path cost 4,Port priority 128.

Designated bridge priority:8,address:80:00:00:0c:fe:00.

Designated port:4,path cost:0.

Ethernet 5 is Forwarding.

Port path cost 4,Port priority 128.

Designated bridge priority:8,address:80:00:00:0c:fe:00.

Designated port:5,path cost:0.

Ethernet 6 is Forwarding.

Port path cost 4,Port priority 128.

-- More --

对于上面的设置结果，可以用 no 命令取消。

Switch#**no set port** 1-3 **spanning-tree port-priority**

Successfully set port priority to default.

Switch#

可以看到进行取消操作后的结果：

Switch#**show spanning-tree ethernet**

Designated root priority:8, address:82:35:00:40:47:00

Ethernet port 1's stp is disable.

Port path cost 10,Port priority 10.

Designated port is 0,path cost:0.

Ethernet port 2's stp is disable.

Port path cost 10,Port priority 10.

Designated port is 0,path cost:0.

Ethernet port 3's stp is disable.

Port path cost 10,Port priority 10.

Designated port is 0,path cost:0.

Ethernet port 4's stp is disable.

Port path cost 10,Port priority 128.

Designated port is 0,path cost:0.

Ethernet port 5's stp is disable.

Port path cost 10,Port priority 128.

Designated port is 0,path cost:0.

Ethernet port 6's stp is disable.

Port path cost 10,Port priority 128.

Designated port is 0,path cost:0.

Ethernet port 7's stp is disable.

Port path cost 10,Port priority 128.

Designated port is 0,path cost:0.

Ethernet port 8's stp is disable.

-- More --

5.3.9.2 基本STP设置命令

对于 STP 的基本设置包括：

- 使能或者关闭 STP
- 配置指定的 STP 参数

使能 STP

【命令格式】spanning-tree enable

【使用指南】该命令用于使能 STP,无参数。

【举例】

Switch(config)#**spanning-tree enable**

Successfully enable spanning tree protocol.

Switch(config)#

禁止 STP

【命令格式】 spanning-tree disable

【使用指南】从系统全局禁止 STP 协议运行，无参数。

【举例】

Switch(config)#**spanning-tree disable**

Successfully disable spanning tree protocol.

Switch(config)#

设置 forward-time 命令

用户执行该命令用于设置 STP 的转发时间。

【命令格式】1. spanning-tree forward-time <400-3000>

2. no spanning-tree forward-time

【使用指南】该命令 1 能设置成 4 到 30 秒中的一个值。在从阻塞状态转换到转发状态时，这是任何交换机端口在侦听情况下所花费的时间。命令 2 恢复 forward time 的缺省值，缺省值为 15S。

【参数说明】<400-3000>为转发延迟大小，单位为 1/100 秒。

注意：当用户欲变动生成树参数时，请一定记住下述公式：

最大的桥老化时间<=2×（桥转发时延－1 秒）

即：Max.Age <=2×(Forward Delay-1)

最大的桥老化时间>＝2×（呼叫时间＋1 秒）

即：Max.Age>=2×（Hello Time+1）

【举例】

Switch(config)#**spanning-tree forward-time** 2400

Successfully set forward delay time.

Switch(config)#

Switch(config)# **no spanning-tree forward-time**

Successfully set forward delay time to default.

Switch(config)#

设置 hello-time 命令

设置当本交换机被选为根桥时发送BPDU 的时间间隔。

【命令格式】1. spanning-tree hello-time <100-1000>

2. no spanning-tree hello-time

【使用指南】Hello Time 能被设置为从 1 到 10 秒中的一个值。这是根网桥发送两个通知其它交换机它是根网桥的 BPDU 包的发送时间间隔。命令 2 恢复 hello time 的缺省值，缺省值为 1S。

【参数说明】<100-1000>为呼叫时间大小，单位为 1/100 秒。

注意：当用户欲变动生成树参数时，请一定记住下述公式：

最大的桥老化时间<=2×（桥转发时延－1 秒）

即：Max.Age <=2×(Forward Delay-1)

最大的桥老化时间>＝2×（呼叫时间＋1 秒）

即：Max.Age>=2×（Hello Time+1）

【举例】

Switch(config)#**spanning-tree hello-time** 500

Successfully set hello time.

Switch(config)#

Switch(config)#**no spanning-tree hello-time**

Successfully set hello time to default.

Switch(config)#

设置报 max-age 命令

设置BPDU 报文老化的最长时间间隔，收到超过这个时间的BPDU 报文，就直接丢弃。

【命令格式】1. spanning-tree max-age <600-4000>

2. no spanning-tree max-age

【使用指南】Max. Age 能被设置为从 6 到 40 秒中的一个值。在 Max. Age 结束时，如果仍没有从根网桥接收到一个 BPDU,你的交换机将开始发送它自己的 BPDU 给其它所有交换机来确定成为根网桥。命令 2 恢复 max age 的缺省值，缺省值为 20S。

设置 STP max age。

注意：当用户欲变动生成树参数时，请一定记住下述公式：

最大的桥老化时间<=2×（桥转发时延－1 秒）

即：Max.Age <=2×(Forward Delay-1)

最大的桥老化时间>＝2×（呼叫时间＋1 秒）

即：Max.Age>=2×（Hello Time+1）

【举例】

Switch(config)#**spanning-tree max-age** 3000
Successfully set max age.
Switch(config)#
Switch(config)#**no spanning-tree max-age**
Sucessfully set max age to default.
Switch(config)#

设置 priority 命令

用户执行该命令用于设置本交换机的优先级。

【命令格式】1. spanning-tree priority <0-65535>

2. no spanning-tree priority

【使用指南】命令 1 为交换机设定的 Priority，能设置成 0 到 65535 中的一个数值。命令 2 恢复 STP priority 的缺省值，缺省值为 32768。

【参数说明】优先级数值。

【举例】

Switch(config)#**spanning-tree priority** 4000

Successfully set priority.

Switch(config)#

Switch(config)# **no spanning-tree priority**

Successfully set priority to default.

Switch(config)#

可以使用 show spanning-tree protocol 命令显示设置的结果。

Switch#**show spanning-tree protocol**

Spanning tree is executing the IEEE compatible Spanning Tree protocol.

Bridge Identifier has priority 32768, address 00:40:47:00:00:00.

Configured hello time 200, max age 2000, forward delay 2000.

Current root has priority 32768, address 00:40:47:00:00:00.

Root port is 0, cost of root path is 0.

Hold time: 1(s),topology change 1.

Switch#

5.3.10 认证设置

5.3.10.1 设置802.1x

关于 802.1x 的使能和禁止包括对于设备和端口的 802.1x 操作。

使能 802.1x

【命令格式】set dot1x enable

【使用指南】用户执行该命令从全局允许 802.1x 功能。

【举例】

Switch#**set dot1x enable**

802.1x protocol are enabled.

Switch#

禁止 802.1x

【命令格式】set dot1x disable

【使用指南】用户执行该命令从全局允许 802.1x 功能。

【举例】

Switch#**set dot1x disable**

802.1x protocol are disabled.

Switch#

使能端口的 802.1x

【命令格式】set port <portlist|all> dot1x enable

【使用指南】用户执行该命令来允许端口的 802.1x 功能。

【参数说明】<portlist|all>为交换机物理端口列表，输入的形式可以是“ 1－2 ”或者“ 1，2，4－6 ”，如果要设置全部的物理端口可以使用 “ all ” 参数项。

【举例】

Switch#**set port** all **dot1x enable**
Successfully enable ports' 802.1x functions.
Switch#

禁止端口的 802.1x

【命令格式】set port <portlist|all> dot1x disable

【使用指南】用户执行该命令来禁止端口的 802.1x 功能。

【参数说明】<portlist|all>为交换机物理端口列表，输入的形式可以是“ 1－2 ”或者“ 1，2，4－6 ”，如果要设置全部的物理端口可以使用 “ all ” 参数项。

【举例】

Switch#**set port** all **dot1x disable**
Successfully forbidden ports' 802.1x functions.
Switch#

5.3.10.2 配置radius服务

使用 radius 认证服务包括两个方面的设置，即 radius 客户端配置和 radius 服务器端配置。在

使用中，把 es3326 作为客户端，所以在配置的时候，选取的客户端的 ip 地址只能是在交换机上配置的一个 supervlan 的地址。Radius 服务器可以有多个，是一个不同的 id 来进行标识。

配置 radius 客户端

配置 radius 客户端的 ip 地址

用户执行该命令对 radius client 的 IP 地址进行配置。

【命令格式】radius client ip <A.B.C.D>

【使用指南】radius client 的 IP 地址往往为某个 supervlan 接口的 IP 地址。

【参数说明】<A.B.C.D>为点分十进制表示的 IP 地址,参数的设定范围只能是设定的某个 supervlan 的 ip，否则设置不成功。

【举例】

Switch(config)#**radius client ip** 192.168.32.11
Successfully set radius address.
Switch(config)#

配置加密算法

用户执行该命令设置在客户端使用的加密算法类型。

【命令格式】radius client encrypt <CHAP|PAP>

【使用指南】目前 radius 协议只支持两种加密算法，CHAP 和 PAP。

【参数说明】<CHAP|PAP>为目前支持的加密算法的类型。

【举例】

Switch(config)#**radius client encrypt** chap

Successfully set radius encrypting method.

Switch(config)#

配置认证端口号

该命令设置 radius client 侧的接收认证报文的应用层端口号。

【命令格式】radius client port authen <1024-65535>

【参数说明】<1024-65535>为应用层端口号。

【举例】

Switch(config)#**radius client port authen** 1812

Successfully set radius account receive port.

Switch(config)#

配置计费端口号

该命令设置 radius client 侧的接收计费报文的应用层端口号。

【命令格式】radius client port account <1024-65535>

【参数说明】<1024-65535>为应用层端口号

【举例】

Switch(config)#**radius client port account** 1813

Successfully set radius account receive port.

Switch(config)#

显示基本 RADIUS 基本配置命令

可以使用 show radius client 命令查看配置的结果

Switch#**show radius client**

RADIUS client IP address . . . . . . ….. .: 192.168.32.11
RADIUS client authentication port. . . .: 1812
RADIUS client account port . . . . ….: 1813
RADIUS client encrypting method. . . ..: chap
Switch#

配置 radius 服务器

在当前配置提示符下键入”radius server”进入对 radius server 的相关信息进行配置。

【命令格式】

1.radius server id <1-6> ip <A.B.C.D> port <1024-65535> secret <key> retrans <1-5> interval <10-1000> type <authen,account,authen&account>

2. no radius server id <1-6>

【使用指南】命令 1 用于添加一个 radius server。”id”是 radius server 过程中比不可少的一项配置命令。命令 2 为删除一个 radius server，该命令的参数指明 radius server 的 ID 号。

【参数说明】<1-6>为 server 的 ID 号；<A.B.C.D>为点分十进制方式表示的 SERVER 的 IP 地址；<1024-65535>是 radius server 接收报文的应用层端口号，如果接收认证报文缺省端口号为 1812。如果接收计费报文缺省端口号为 1813；<key>为为长度在 3-128 之间的字符串，用来标识 client 和 server 之间的共享密钥；<1-5>为用于配置 radius client 向 radius server 发送报文的最大重传次数，缺省值为 3；<10-1000>为 radius client 向 radius server 发送报文时，没收到 server 的响应而进行重传的最大时间间隔，缺省值为 10S，单位为秒；<authen,account,authen&account>是 server 接收报文的类型，目前 server 只支持三种类型：authentication，accounting，authentication and accounting，分别用 “ authen,account,auth&account ” 来表达。

【举例】

Switch(config)#**radius server id** 1 **ip** 192.168.32.100 **port** 1024 **secret** tp **retrans** 1 **interval** 100 **type** authen

Successfully configure a RADIUS server.

Switch(config)#

注意：Radius Server IP 地址应该和本地设备带内口 IP 地址处于一个网段，并且连接端口为不需认证，因此在预置 1/2/3/4 口连接非认证设备，5/6/7/8 端口连接认证设备。非认证设备不需拨号就可以接入，而认证端口必须拨号。Radius server 所在主机连接在 1/2/3/4 端口之一，待认证主机接至 5/6/7/8 端口之一。

查看 server 配置命令

可以使用命令 show radius server 显示关于 radius server 的配置信息。

Switch#**show radius server**

Id	IpAddress	Port	Times	Interval	Secret	Type
1	192.168.32.100	1	3	100	tp	authentication

Switch#

5.3.11 ACL设置

该命令可以实现如下的功能：报文过滤条件的添加和删除，可以实现 mac＋ip＋port 的绑定，可以实现用户的带宽控制，最小粒度为 1M，步长为 1M；静态组播表项的添加和删除；单播表项的添加和删除；

5.3.11.1 multicast-forwarding命令

用户执行该命令配置多播转发表项

【命令格式】1. access-list multi-forward mac-addr < HH:HH:HH:HH:HH:HH > vid <1-4094>

memberport <portlist> cos [0-7]

2. no accesslist multi-forward mac-address < HH:HH:HH:HH:HH:HH > vid <1-4094>

【使用指南】命令 1 添加一个多播表项；

命令 2 删除一个多播表项。

【参数说明】< HH:HH:HH:HH:HH:HH >为 mac 地址；<1-4094> 为 vlan 标识，取值范围为 1－4094；<portlist>是端口列表，用“ xx-xx ”格式表示，“ xx ”表示端口号；[0-7]为 cos 值，取值为 0－7，该参数可选。

【举例】

Switch(config)#**access-list multi-forward mac-addr** 01:01:01:0f:0c:0d **vid** 1 **memberport** 1-5 **cos** 1

Successfully set static multicast cos value.

Switch(config)#

可以使用下面的命令显示设置的结果

Switch#**show access-list mutli-forward**

```
********************Access list multi-forward*********************
  MacAddress          Vid   Mport   Cos   Type
  01:01:01:0f:0c:0d    1     1-5     1     access list
```

Switch#

使用下面的命令来取消上面的设置。

Switch(config)#**no accesslist multi-forward mac-addr** 01:01:01:0f:0c:0d **vid** 1

Successfully delete the static multicast.

Switch(config)#

5.3.11.2 uni-forward命令

用户执行该命令配置单播转发表项

【命令格式】1. access-list uni-forward mac-addr < HH:HH:HH:HH:HH:HH > vid <1-4094> action <forward|drop-src|drop-dst> port <1-8> attribute [cos-src<0-7>|cos-dst<0-7>]

2. no accesslist uni-forward mac-address < HH:HH:HH:HH:HH:HH > vid <1-4094>

【使用指南】命令 1 添加一个单播表项；

命令 2 删除一个单播表项。

【参数说明】< HH:HH:HH:HH:HH:HH >为 mac 地址；<1-4094> 为 vlan 标识；<forward|drop-src|drop-dst> 为设置的单播表项所采取的策略；<1-8> 是端口号；[cos-src<0-7>|cos-dst<0-7>]为 Cos 属性值，可以选择基于源的也可以选择基于目的的 cos 值。

【举例 1】如何实现 mac＋port 的绑定？

Switch(config)#**access-list uni-forward mac-addr** 01:01:01:0f:0c:0d **vid** 1 **action forward port** 1 **attribute**

Successfully set the static arl table.

Switch#**show access-list uni-forward**

*********************Access list uni-forward*********************

Action	MacAddress	Vid	Port	Cos	Cod	Status
forward	ff:ff:ff:ff:ff:fe	4094	1	0	0	static
forward	ff:ff:ff:ff:ff:ff	1	28	0	0	static
forward	01:01:01:0f:0c:0d	1	1	0	0	static
forward	00:40:47:00:00:08	1	28	0	0	static
forward	00:40:47:00:00:07	1	28	0	0	static

forward	00:40:47:00:00:06	1	28	0	0	static
forward	00:40:47:00:00:05	1	28	0	0	static
forward	00:40:47:00:00:04	1	28	0	0	static
forward	00:40:47:00:00:03	1	28	0	0	static
forward	00:40:47:00:00:02	1	28	0	0	static
forward	00:40:47:00:00:01	1	28	0	0	static
forward	00:40:47:00:00:00	1	1	0	0	static

Switch#

这样你就将 mac 01:01:01:0f:0c:0d 和 port 1 绑定了。

【举例 2】

Switch(config)#**access-list uni-forward mac-addr** 01:01:01:0f:0c:0d **vid** 1 **action forward port** 1 **attribute cos-src** 1

Successfully set the static arl table.

Switch(config)#**no accesslist uni-forward mac-addr** 01:01:01:0f:0c:0d **vid** 1

Successfully delete the static unicast arl table.

Switch(config)#

5.3.11.3 packet-filter命令

用户执行该命令配置过滤条件，系统提供的过滤功能是基于单个数据报的。对于到达的每一个数据报，系统会和过滤表中的表项进行匹配，如果找到匹配的表项，根据该过滤表项设定的策略，如果是“ deny ”的一个过滤表项，就会丢弃该数据报；如果是“ permit ”的一个过滤项，则转发或者上送该数据报。

系统提供基于多种过滤条件的设置，包括既根据指定端口号、源/目的 MAC、源/目的 IP 地址、源/目的应用层端口号。**从而可以实现端口，与 ip 地址，mac 地址，或者协议的绑定。**

【命令格式】1. a access-list packet-filter id <1-200> action <permit|deny> rule [….]

2. no accesslist packet-filter id <1-200>

3 no accesslist packet-filter all

【使用指南】命令 1 添加一个包过滤表项；

命令 2 删除一个包过滤表项。

命令 3 删除所有设置项。

【参数说明】<1-200> 是添加的过滤表项的标识，<permit|deny>为添加的过滤表项的策略，另外的可选参数包括

inport	<1-8> Ingress Physical Port Number
eport	<1-8> Egress Physical Port Number
destmac	<HH:HH:HH:HH:HH:HH> Destination Mac Address
destip	<A.B.C.D> Destination Ip Address
dest-submask	<A.B.C.D> Destination Mask Address
dest-app-port	<1-65535> Destination Application Port Number
srcmac	<HH:HH:HH:HH:HH:HH> Source Mac Address
srcip	<A.B.C.D> Source Ip Address
src-submask	<A.B.C.D> Source mask Address
src-app-port	<1-65535> Source Application Port Number

注意：

1．如果设置的策略会带来冲突，设置不成功。比如针对一个端口或者 ip 设置了“ deny ”的策略，如果再对该端口或者 ip 设置“ permit ”策略，就会不成功。

2．在设置匹配策略的时候要注意，对于过滤条目的匹配是完全匹配，如果没有匹配的项或者只有部分项匹配，对于该数据报的处理将会按照默认的策略执行。

【举例】

Switch(config)#**access-list packet-filter id** 1 **action** deny **rule inport** 1

Successfully set the filter.

Switch(config)#

可以使用下面的命令显示设置的结果

Switch#**show access-list packet-filter**

```
********************Access list packet filter*********************
* S=source D=destination P=permit F=forbidden E=egress I=input        *
************************************************************
Id Act   Port   MacAddress             IpAddress              APort
1   P    1(I)
Switch#
```

Switch(config)#**no accesslist packet-filter id** 1

Successfully delete the filter1.

Switch(config)#

Switch(config)#**no accesslist packet-filter all**

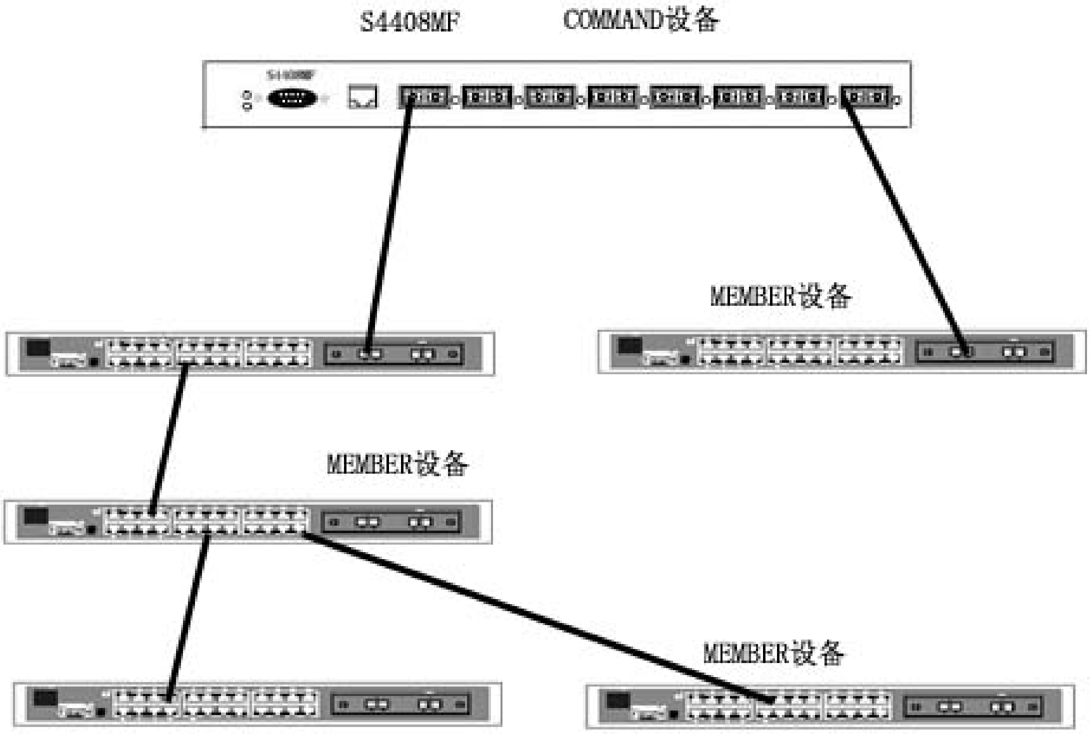
Successfully delete all the filter

Switch(config)#

5.3.12 集群管理

5.3.12.1 ddp命令

设备发现协议配置，该协议也用于集群管理



集群管理拓扑示意图

如图所示，可以使用选定的命令设备来管理其它的设备。实现集群管理的操作步骤为：

- 把要进行管理的设备和选定的命令设备进行正确的拓扑连接。
- 使能所有设备的 ddp 协议。
- 为作为一个域进行管理的设备分配一个域名，只有同属于一个域的设备才能完成管理功能。
- 为要进行远程管理的设备创建一个有管理员操作权限的用户。
- 把选定的 command 设备设为 ddp 的 master 设备。

- 如果这时连接成功，可以在 command 设备上执行 show ddp neighbor 命令显示和该 command 设备处于同一域中的设备。
- 对于可以被 ddp 发现的设备就可以通过 command 设备来进行管理。

使能 ddp

用户执行该命令打开当前设备的 ddp 功能，使当前设备能够进行集群管理。

【命令格式】ddp enable

【参数说明】无

【举例】

Switch(config)#**ddp enable**
DDP protocol are enabled
Switch(config)#

禁止 ddp

用户执行该命令关闭当前设备的 ddp 功能，当前设备不再具有集群管理的特性。

【命令格式】ddp disable

【参数说明】无

【举例】

Switch(config)#**ddp disable**
DDP protocol are disabled.
Switch(config)#

配置 ddp 域名

设置当前设备的 ddp domain name。

【命令格式】ddp domain-name <name>

【参数说明】<name>为最大长度为 256 的字符串，用来表示 domain 的名称，最好用””括起来

【举例】

Switch(config)#**ddp domain-name** "domain1”

DDP domain name set to domain1

Switch(config)#

设置 ddp 命令设备

用户执行该命令设置当前设备为 ddp command 设备。

【命令格式】ddp master

【参数说明】无

【举例】

Switch(config)#**ddp master**

Switch(config)#

设置 ddp 监听设备

用户执行该命令设置当前设备为 ddp 监听设备。

【命令格式】no ddp master

【参数说明】无

【举例】

Switch(config)# **no ddp master**

Switch(config)#

显示 ddp 基本信息

用户执行该命令显示设备的 ddp 状态和参数。

【命令格式】show ddp summary

【参数说明】无

【举例】

Switch#**show ddp summary**

DDP protocol is enable.DDP domain name is: domain1.

Switch#

显示 ddp 从设备

用户执行该命令显示 ddp 发现的其他设备。

【命令格式】show ddp neighbor

【参数说明】无

【举例】

Switch#**show ddp neighbor**

Device	Port	Mac Address	L3 Address	Cluster	Type	Time
sample	sy42949	00:0c:fe:00:00:e0	0.0.0.0	0	L3switch&agent	0

5.3.12.2 cluster命令

使能命令设备

该命令设置当前的设备为 cluster 的命令设备。

【命令格式】cluster enable <devicename>

【参数说明】<devicename>为最大长度为 256 的字符串，用于表示命令设备的名称

【举例】

Switch(config)#**cluster enable** “manager”

Successfully set to a command device.

Switch(config)#

禁止命令设备

如果当前设备是 cluster 的命令设备，该命令把当前设备从命令状态转换到候选状态。

【命令格式】cluster disable

【参数说明】无

【举例】

Switch(config)#**cluster disable**

Successfully set to candidate status.

Switch(config)#

设置候选设备

该命令设置当前的设备为 cluster 的候选设备。

【命令格式】cluster candidate

【参数说明】无

【举例】

Switch(config)#**cluster candidate**
Successfully set the device to candidate device.
Switch(config)#

禁止候选设备

如果当前设备是 cluster 的 member 设备，把当前设备直接设置为候选设备，相当于静态设置。这个命令生效后，此时 command 设备并不知晓这个 member 设备状态的改变，它已经不再属于 cluster 了。

【命令格式】cluster change candidate

【参数说明】无

【举例】

Switch(config)#**cluster change candidate**
Switch(config)#

设置独立设备状态

该命令设置当前的设备为 cluster 的独立设备，也就是此设备不可以被 command 设备添加到自己

的 cluster 中。

【命令格式】cluster independent

【参数说明】无

【举例】

Switch(config)#cluster independent
Successfully set to independent.
Switch(config)#

添加/删除成员设备

如果当前设备是 cluster 的命令设备，该命令用于添加/删除 cluster 中的 member 设备。

【命令格式】1.cluster add <devicename>1 username <name> password <password>

2. no cluster <devicename>

【使用指南】如果当前设备是 cluster 的命令设备，命令 1 用于把其他当前状态是候选状态的设备添加到 cluster 中，命令 2 用于把其中的 member 设备从 cluster 中删除。

【参数说明】<devicename>为对方设备的名称；<name>为该超级用户名，为一字符串; <password>为对方设备的一个超级用户的密码，为一个字符串。

注意：

1. **使用的用户名和口令参数必须存在，使用的设备名必须是用“show ddp neighbor”显示的设备名。**
2. **在执行上述命令时，command 设备需要使用一个具有管理员权限的用户进行操作，而不能是系统默认的“admin”管理员帐户。**

【举例】

Switch(config)#**cluster add** “devicename” **username** "slave" **password** "pass"

Successfully add a member.

Switch(config)#

改变成员状态

把当前设备直接设置为某个 cluster 的 member 设备，相当于静态设置。这个命令生效后，command 设备并不知晓这个 member 设备，但是 member 设备把 command 设备当作 cluster 的 command 设备。

【命令格式】cluster change member name <clustername> mac-addr <HH:HH:HH:HH:HH:HH>

【参数说明】<clustername>为最大长度为 256 的字符串，用于表示 cluster 的名称，<HH:HH:HH:HH:HH:HH>为 cluster 中命令设备的 MAC 地址。

【举例】

Switch(config)#**cluster change membe**r **name** “cluster1” **mac-addr** 00:02:e3:45:62:f5

Switch(config)#

show cluster summary

用户执行该命令显示当前设备的 cluster 状态和参数。

【命令格式】show cluster summary

【参数说明】无

【举例】

Switch#**show cluster summary**

Cluster name is:manager

Device is cluster Command status.

Switch#

show cluster member

如果当前设备是 cluster command 设备，此命令用于显示，当前所有的 member 成员。

【命令格式】show cluster member

【参数说明】无

【举例】

Switch#**show cluster member**

Cluster name is:manager

Device is cluster Command status.

Switch#

远程管理命令 rcommand

rcommand 命令用于实现设备的远程管理，需要两台以上的交换机，其功能类似于 telnet 网管方式。rcommand 是通过 ulink 协议进行传输，所以这里的 rcommand 命令有节省 IP 地址的优点。另外和 telnet 不同之处是 Telnet 需要客户端对收到的报文进行解释，而我们的 rcommand 命令的主要功能是透传，解释功能还是由 console 终端或者 Telnet 终端完成。

【命令格式】rcommand <name>

【参数说明】<name>另一台交换机的设备名称，为一字符串。

注意：在使用 rcommand 前要求进行控制和被控制的设备的 ddp 协议均被使能，并且把

设备加入到同一个域中，同时把进行控制的设置设置为 ddp 命令设备。这样被控制设备作为进行控制的设备的从设备，可以使用显示从设备的命令进行显示，只有在显示结果中可以看到从设备，才可以成功执行 rcommand 命令。

【举例】

假设有下面两个设备。

设备名称	提示符	超级用户名	密码	举例
设备 A：	deviceA	tpA	tpA	图表 1
设备 B：	deviceB	tpB	tpB	图表 2

```
deviceA#
deviceA# show user
User name      Password       Access level      Property
__________     ___________    _____________     _________
tpA            tpA            15                 0
```

图表 1

```
deviceB#
deviceB# show user
User name      Password       Access level      Property
__________     ___________    _____________     _________
tpB            tpB            15                 0
```

图表 2

在设备 A 上执行命令 rcommand 命令后结果如下：

```
deviceA#
deviceA#rcommand deviceB
login：tpB
password：
deviceA#deviceB#show user
User name     Password      Access level     Property
__________    ___________   _____________    _________
tpB           tpB           15                0
```

deviceA#rcommand deviceB 提示符后面的命令是当前设备 B 上的命令，和在设备 B 上执行的命令完全相同。

5.3.13 配置igmp

5.3.13.1 设置igmp的版本

【命令格式】ip igmp version <1|2>

【使用指南】该命令用于设置交换机中运行的关于 igmp 的版本，目前的设置可以是版本 1 和 2。

【举例】]

Switch#**configure**

Switch(config)#**interface** 1

Switch(config-if)#**ip igmp version** 2

Switch(config-if)#

5.3.13.2 禁止igmp

【命令格式】no ip igmp

【使用指南】该命令用于禁止 igmp 协议。

【举例】

Switch(config-if)#**no ip igmp**

Switch(config-if)#

5.3.13.3 ip igmp snooping命令

用户执行该命令对 igmp snooping 的相关参数进行配置。

【使用指南】本命令集包括所有 igmp snooping 的配置命令。

aging

用户执行该命令设置 igmp snooping 的老化时间。

【命令格式】1. ip igmp snooping aging <30-3600>

2. no ip igmp snooping aging

【使用指南】命令 2 恢复 igmp snooping 老化时间的缺省值，该命令不带任何参数，缺省值为 300。

【参数说明】<30-3600>为 igmp snooping 的老化时间值，为整形变量。

【举例】

Switch<config ># **ip igmp snooping aging** 100

igmp snooping aging time set to 100

Switch<config ># **no ip igmp snooping aging**

igmp snooping aging time set to 300

Switch<config >#

alert

用户执行该命令设置 igmp snooping alert 功能。

【命令格式】1. ip igmp snooping alert enable

2. ip igmp snooping alert disable

【参数说明】命令 1 使能 alert 功能；命令 2 关闭 alert 功能。

【举例】

Switch(config)#**ip igmp snooping alert enable**

Successfully enable igmp snooping alert.

Switch(config)#

关闭 igmp snooping 功能

用户执行该命令关闭 igmp snooping 功能。

【命令格式】ip igmp snooping disable

【使用指南】该命令无任何参数。

【举例】

Switch(config)#**ip igmp snooping disable**

Successfully disable igmp snooping.

Switch(config)#

激活 igmp snooping 功能

用户执行该命令激活 igmp snooping 功能。

【命令格式】ip igmp snooping enable

【使用指南】该命令无任何参数。

【举例】

Switch<config ># **ip igmp snooping enable**

Successfully enable igmp snooping.

Switch<config >#

显示 igmp snooping 设置

Switch#**show ip igmp snooping**

IGMP snooping is enable.

IGMP snooping aging time is 300

IGMP snooping alert is disable.

Switch#

5.3.14 配置DHCP协议

用户执行该命令进行 DHCP relay 的配置。

5.3.14.1 关闭DHCP relay的功能

用户执行该命令关闭 DHCP relay 的功能。

【命令格式】ip dhcp relay disable

【使用指南】该命令不带任何参数，从全局禁止 DHCP relay 功能。

【举例】

Switch(config)#**ip dhcp relay disable**

Successfully disable DHCP relay..

Switch(config)#

5.3.14.2 使能DHCP relay的功能

用户执行该命令激活 DHCP relay 的功能。

【命令格式】ip dhcp relay enable

【使用指南】该命令不带任何参数，从全局允许 DHCP relay 功能。

【举例】

Switch(config)#**ip dhcp relay enable**

Successfully enable DHCP relay.

Switch(config)#

5.3.14.3 刷新命令

用户执行该命令刷新 DHCP relay 的配置。

【命令格式】ip dhcp relay refresh

【使用指南】这个命令是在 SuperVlan 配置之后，用来刷新和 SuperVlan 相关的 DHCP relay 配置，不带任何参数。

【举例】

Switch<config ># **ip dhcp relay refresh**

Switch<config >#

5.3.14.4 配置DHCP server命令

用户执行该命令增加新的 DHCP Server。

【命令格式】1. ip dhcp relay target Id <1-5> Ipaddress <A.B.C.D>

2. no ip dhcp relay target <1-5>

【使用指南】交换机的 DHCP relay 功能支持多个 DHCP Server，target 命令创建或添加新的 DHCP Server，命令 2 删除存在的 DHCP Server。

【参数说明】<1-5>为本设备上 DHCP server 的编号；<A.B.C.D>为新添加的 DHCP server 的 IP 地址；

【举例】

Switch(config)# **ip dhcp relay target id** 1 **ipaddress** 192.168.32.10

Successfully set dhcp target.

Switch(config)#

Switch(config)# **no ip dhcp relay target** 1

Successfully delete dhcp target.

Switch(config)#

Switch# **show ip dhcp relay**

DHCP status: Disable

Dhcp Server Number:1

Server Id   Ip Address

1   192.168.32.10

Switch#

5.3.15 路由协议

配置路由协议时要先使能一种路由协议，目前 ES3326 支持的路由协议包括 rip 和 ospf 两种。

5.3.15.1 使能路由协议

用户执行该命令来指定路由协议。

【命令格式】router protocol <NULL|rip|ospf>

【参数说明】<NULL|rip|ospf>为路由协议类型，包括三种：

- null 代表无路由协议；
- rip 代表 rip 协议；
- ospf 代表 ospf 协议。

【举例】

Switch(config)#**router protocol rip**

Routing protocol is set to rip.

Switch(config)#

5.3.15.2 配置OSPF

area 命令

用户执行该命令创建/删除一个 area。

【命令格式】1. area <A.B.C.D>

2. no area

【使用指南】area 是由 IP 地址来标识的，命令 2 删除一个 area。

【参数说明】<A.B.C.D>为新创建的 area 的 ip 地址，以点分十进制方式表示。

注意：

1. 使用本命令前请在 router protocol 中使能 OSPF 协议。

2.如果设置的 area 已经在使用，不可以使用删除命令。

【举例】

Switch#**configure**

Switch(config)#**router ospf**

Switch(config-ospf)#**area** 10.1.1.1

Set a new area 10.1.1.1 successfully.

Switch(config-ospf)#

使用下面的命令查看设置的结果

Switch#**show ip ospf area**

Area 10.1.1.1

No area summary

External AS advertisements is allowed

SPF algorithm executed 0 times

Area have 0 ABR and 0

Number of LSA 0

Area LSA Checksum Sum 0x0

Number of interfaces in this area is 0

Switch#

Switch(config-ospf)#**no area** 10.1.1.1

Delete area 10.1.1.1 successfully.

Switch(config-ospf)#

networks 命令

用户执行该命令创建新的网络。

【命令格式】1. networks ip <A.B.C.D> mask<A.B.C.D> area<A.B.C.D>

2. no network ip <A.B.C.D>

【使用指南】网络是由 IP 地址和子网掩码来标识的，命令 2 删除一个 network。

【参数说明】

IP 后面的<A.B.C.D>为新创建的网络的 ip 地址，该地址必须为交换机的 supervlan 的 ip 地址，否则无效

Mask 后面的<A.B.C.D>为新创建的网络的子网掩码，该掩码必须为 ip 地址对应的子网掩码，否则无效

Area 后面的<A.B.C.D>为该新建网络所在的 area 地址，该区域必须已经存在，否则无效

三参数均以点分十进制方式表示。

【举例】

Switch(config-ospf)#**network ip** 192.168.32.11 **mask** 255.255.255.0 **area** 10.1.1.1

Interface 192.168.32.11 was created.

Switch(config-ospf)#

可以使用 show ip ospf interface 来显示设置的结果

Switch#**show ip ospf interface**

Interface address is 192.168.32.11, administrator status is up

State designatedRouter

This interface belong to area 10.1.1.1

Network Type broadcast , Priority 1 , Transmit Delay is 1 sec

Timer intervals configured, Hello 10, Dead 40, Retransmit 5

DR (ID) 192.168.32.11 , Backup DR (ID) 0.0.0.0

Interface event 3 times

Interface Authentication type : no , Authentication ID 1

Interface Authentication key

Interface Cost 1

Switch#

Switch(config-ospf)#**no network ip** 192.168.32.11

Interface 192.168.32.11 was deleted.

Switch(config-ospf)#

5.3.15.3 配置RIP

network 命令

用户执行该命令创建 rip 协议的网络。

【命令格式】1. network <A.B.C.D>

2. no network <A.B.C.D>

【使用指南】新创建的网络由 IP 地址来标识的，命令 2 删除一个网络。

【参数说明】<A.B.C.D>为所创建网络的 IP 地址，以点分十进制方式表示。

注意：在 S4408MF 中该地址必须是一个设定的 supervlan 的 ip 地址，否则设置不成功。

【举例】

Switch(config)#**router rip**

Switch(config-rip)#

Switch(config-rip)#**network** 192.168.32.11

Successfully create rip interface config table.

Switch(config-rip)#

可以使用下面的命令来显示设置的结果

Switch#**show ip rip interface**

IpAddress	Status	SendMode	RecvMode	Metric	AuthenticationType
192.168.32.11	enable	ripVersion2	rip1OrRip2	0	none

Switch#

使用下面的命令来取消上面的设置。

Switch(config-rip)#**no network** 192.168.32.11

Successfully delete rip interface config table.

Switch(config-rip)#

5.3.15.4 基于supervlan的OSPF设置

用户执行该命令对 OSPF 协议的相关参数进行设置。

【使用指南】OSPF 命令包含一个命令集，该命令集定义了对 OSPF 接口操作的相关命令。

注意：在配置 OSPF 之前，必须先使能 OSPF 协议，用“ router protocol ospf ”命令,否则配置会出现失败。

设置认证方式

用户执行该命令设置 ospf interface 的鉴权方式。

【命令格式】1. ip ospf authen <text|message-digest>

2. no ip ospf authen

【使用指南】该接口通过 IP 地址来指定， 命令 2 用于取消鉴权方式（也就是不鉴权），该命令不带任何参数。

【参数说明】：参数为鉴权方式，我们支持 text（simplepassword）和 message-digest 两种方式。

【举例】

Switch#**configure**

Switch(config)#**interface** 1

Switch(config-if)#**ip ospf authen**

<Enumerate> <message-digest/text> Authentication type

<cr>

Switch(config-if)#**ip ospf authen** message-digest

Successfully set ospf authentication type.

Switch(config-if)#**no ip ospf authen**

Successfully clear ospf authentication type.

Switch(config-if)#

设置认证密钥

用户执行该命令设置 ospf interface 鉴权方式的密钥。

【命令格式】1. ip ospf authen-key-id <1-4294967295> key <key>

2. no ip ospf authen-key -id

【使用指南】该接口通过 IP 地址来指定，命令 2 取消设置的密码，就是设置密码为空。

【参数说明】<1-4294967295>为密钥字符串标识，以十进制数方式表示；<key>为长度为 0-256 的密钥字符串，最好用“ ”括起来。

【举例】

Switch(config-if)#**ip ospf authen-key-id** 1 **key** "pass"

Successfully set ospf authentication key.

Switch(config-if)#

Switch(config-if)#**no ip ospf authen-key-id**

Successfully clear ospf authentication key.

Switch(config-if)#

设置接口花销

用户执行该命令设置 ospf interface 的 cost。

【命令格式】1. ip ospf cost <1-65535>

2. no ip ospf cost

【使用指南】该接口通过 IP 地址来指定，命令 2 用于恢复 cost 的缺省值,缺省值为 1。

【参数说明】<1-65535>为 dead-interval 时间间隔，单位为秒。

【举例】

Switch(config-if)#**ip ospf cost** 50

Successfully set ospf cost.

Switch(config-if)#

Switch(config-if)#**no ip ospf cost**

Successfully clear ospf cost.

Switch(config-if)#

设置 dead-interval

用户执行该命令设置 ospf interface 的 dead-interval。

【命令格式】1. ip ospf dead-interval <1-65535>

2. no ip ospf dead-interval

【使用指南】命令 2 用于恢复 dead-interval 的缺省值,缺省值为 40S。

【参数说明】<1-65535>为 dead-interval 时间间隔，单位为秒。

【举例】

Switch(config-if)#**ip ospf dead-interval** 30

Successfully set ospf dead interval.

Switch(config-if)#

Switch(config-if)#**no ip ospf dead-interval**

Successfully set ospf dead interval.

Switch(config-if)#

设置呼叫间隔

用户执行该命令设置 ospf interface 的呼叫间隔 hello-interval。

【命令格式】1. ip ospf hello-interval <1-65535>

2. no ip ospf hello-interval

【使用指南】命令 2 用于恢复呼叫间隔的缺省值,缺省值为 10S。

【参数说明】<1-65535>为 hello-interval 时间间隔，单位为秒。

【举例】

Switch(config-if)#**ip ospf hello-interva**l 20

Successfully set ospf hello interval.

Switch(config-if)#

Switch(config-if)#**no ip ospf hello-interval**

Successfully clear ospf hello interval.

Switch(config-if)#

设置网络类型

用户执行该命令设置 ospf interface 的网络类型。

【命令格式】1. ip ospf network <broadcast/non-broadcast/point-to-point/point-to-multipoint>

2. no ip ospf network

【使用指南】命令 2 用于恢复 network 类型的缺省值。

【参数说明】<broadcast/non-broadcast/point-to-point/point-to-multipoint>为网络类型，我们支持下列类型的网络：

broadcast	Specify OSPF broadcast multi-access network
non-broadcast	Specify OSPF NBMA network
point-to-multipoint	Specify OSPF point-to-multipoint network
point-to-point	Specify OSPF point-to-point network

【举例】

Switch(config-if)#**ip ospf network broadcast**

Successfully set ospf network type.

Switch(config-if)#

Switch(config-if)# **no ip ospf network**

Successfully clear ospf network type.

Switch(config-if)#

设置接口优先级

用户执行该命令设置 ospf interface 的优先级。

【命令格式】1. ip ospf priority <0-255>

2. no ip ospf priority

【使用指南】命令 2 用于恢复优先级的缺省值。

【参数说明】<0-255>为该接口的优先级。

【举例】

Switch(config-if)#**ip ospf priority** 100

Successfully set ospf priority.

Switch(config-if)#

Switch(config-if)#**no ip ospf priority**

Successfully set ospf interface default priority.

Switch(config-if)#

设置重传间隔

用户执行该命令设置 ospf interface 重发 LSA 报文的时间间隔。**目前该命令不可配置。**

【命令格式】1. ip ospf retx-interval <1-65535>

2. no ip ospf retx-interval

【使用指南】命令 2 用于恢复重传时间间隔的缺省值，缺省值为 5S。

【参数说明】<1-65535>为 retransmit-interval 时间间隔，单位为秒。

【举例】

Switch<config-if >#**ip ospf retx-interval** 8

Successfully set ospf retransmit interval.

Switch<config-if ># **no ip ospf retx-interval**

Successfully clear ospf retransmit intervall.

Switch<config-if >#

设置传输延迟

用户执行该命令设置 ospf interface 发送 LSA 报文的传输延迟。

【命令格式】1. ip ospf tx-delay <1-65535>

2. no ip osfp tx-delay

【使用指南】该接口通过 IP 地址来指定，命令 2 用于恢复传输延迟的缺省值，缺省值为 1S。

【参数说明】<1-65535>为传输延迟的时间，单位为秒。

【举例】

Switch(config-if)#**ip ospf tx-delay** 3
Successfully set ospf transmit delay.
Switch(config-if)#
Switch(config-if)# **no ip ospf tx-delay**
Successfully clear ospf transmit delay.
Switch(config-if)#

5.3.15.5 基于supervlan的RIP设置

用户执行该命令对 RIP 协议的相关参数进行设置。

【使用指南】RIP 命令包含一个命令集，该命令集定义了对 RIP 接口操作的相关命令。

注意：在配置 RIP 之前，必须先使能 RIP 协议，用“ router protocol rip ”命令,否则配置会出现失败。

设置认证方式

用户执行该命令设置 RIP 接口的鉴权方式。

【命令格式】1. ip rip authen mode <text/md5>

2. no ip rip authen mode

【使用指南】该接口通过 IP 地址来指定，命令 2 用于取消鉴权方式（也就是不鉴权）。

【参数说明】< text/md5>为鉴权方式，我们支持 text（simplepassword）和 md5 两种方式。

【举例】

Switch(config-if)#**ip rip authen mode** md5

Successfully set rip authentication type.

Switch(config-if)#

Switch(config-if)# **no ip rip authen mode**

Successfully clear rip authentication type.

Switch(config-if)#

设置认证密钥

用户执行该命令设置 RIP 接口的鉴权密钥。

【命令格式】1. ip rip authen keyid <1-65535> key <key>

2. no ip rip authen key

【使用指南】该接口通过 IP 地址来指定，命令 2 用于取消鉴权密钥。

【参数说明】<1-65535>密钥标识，以十进制数方式表示；<key>为长度为 0-16 的字符串，表示 RIP 协议的密钥，最好用“ ”括起来。

【举例】

Switch(config-if)#**ip rip authen key-id** 1 **key** "pass"

Successfully set rip authentication key.

Switch(config-if)#

Switch(config-if)#**no ip rip authen key**

Successfully clear rip authentication key.

Switch(config-if)#

设置接收版本

用户执行该命令设置 RIP 接口所能接收的 RIP 协议报文的版本号。

【命令格式】1. ip rip receive version <rip1/rip2/rip1orrip2/noreceive>

2. no ip rip receive version

【使用指南】该接口通过 IP 地址来指定，可以选择的设置参数是 rip1,rip2,rip1orrip2,noreceive。分别用于表示版本 1，版本 2，版本 1 或者版本 2，最后一个选项是不接收任何报文。命令 2 设置 rip 接口不接收任何报文。

【参数说明】<rip1/rip2/rip1orrip2/noreceive>为设置 rip 接口可以接受的 rip 报文版本号。

【举例】

Switch(config-if)#**ip rip receive version rip**1

Successfully set rip receive version.

Switch(config-if)#

Switch(config-if)#**no ip rip receive version**

Successfully clear rip receive version.

Switch(config-if)#

设置发送版本

用户执行该命令设置 RIP 接口所能发送的 RIP 协议报文的版本号。

【命令格式】1. ip rip send version <nosend/rip1/rip1compatible/rip2>

2. no ip rip send version

【使用指南】该接口通过 IP 地址来指定，可以选择的选项是 nosend,rip1,rip1compatible,rip2，分别表示不发送，版本 1，版本 1 兼容（这种报文的目的地址是广播地址，而在报文中加入的版本号为版本 2），版本 2。命令 2 设置 rip 接口不发送任何报文。

【参数说明】<nosend/rip1/rip1compatible/rip2> 为设置 rip 接口可以接受的 rip 报文版本号。

【举例】

Switch(config-if)#**ip rip send version rip**2

Successfully set rip send version.

Switch(config-if)#

Switch(config-if)#**no ip rip send version**

Successfully clear rip send version.

Switch(config-if)#

5.3.16 Garp协议

5.3.16.1 设置garp协议定时器

设置 join 定时器

该命令用于设置 garp join timer 的值。

【命令格式】1 .set port <portlist|all> garp join-time<20-20000>

2. no set port <portlist|all>garp join-time

【使用指南】命令 1 用于设置 garp join timer 的值；命令 2 恢复 garp join timer 的缺省值，只需一个参数指明物理端口号即可，缺省值为 20ms。

【参数说明】<portlist|all>为交换机物理端口列表，输入的形式可以是“1－2”或者“1，2，4－6”，如果要设置全部的物理端口可以使用“all”参数项；<20-20000>为该端口的 garp join timer 时间值，单位为 1/100 秒，取值范围为 20－20000。

【举例】

Switch#**set port** all **garp join-time** 200
Successfully set ports' garp join timer.
Switch#
Switch#**no set port** all **garp join-time**
Successfully set garp join time to default.
Switch#

leave 命令

该命令用于设置 garp leave timer 的值。

【命令格式】1.set port <portlist|all> garp leave-time<60-20000>
2. no set port <portlist|all>garp leave-time

【使用指南】命令 1 用于设置 garp leave timer；命令 2 恢复 garp leave timer 的缺省值，只需一个参数指明物理端口号即可,缺省值为 60ms。

【参数说明】<portlist|all>为交换机物理端口列表，输入的形式可以是“1－2”或者“1，2，4－6”，如果要设置全部的物理端口可以使用“all”参数项；<60-20000>为该端口的 garp leave timer 时间值，单位为 1/100 秒，取值范围为 60－20000。

【举例】

Switch#**set port** all **garp leave-time** 100
Successfully set ports' garp leave time.

Switch#

Switch#**no set port** all **garp leave-time**

Successfully set port garp leave time to default.

Switch#

leaveall 命令

该命令用于设置 garp leaveall timer 的值。

【命令格式】1.set port <portlist|all> garp leaveall-time<1000-1500>

2. no set port <portlist|all>garp leaveall-time

【使用指南】命令 1 用于设置 garp leaveall timer 的值；命令 2 恢复 garp leaveall timer 的缺省值，只需一个参数指明物理端口号即可，缺省值为 1000ms。

【参数说明】<portlist|all>为交换机物理端口列表，输入的形式可以是“1－2”或者“1，2，4－6”，如果要设置全部的物理端口可以使用“all”参数项；<1000-1500>为该端口的 garp leaveall timer 时间值，单位为 1/100 秒，取值范围为 1000-1500。

【举例】

Switch#**set port** all **garp leaveall-time** 1200

Successfully set port garp leaveall time.

Switch#

Switch#**no set port** all **garp leaveall-time**

Successfully set ports' garp leaveall time to default.

Switch#

可以用下面的命令显示 garp 设置的结果。也可以用 show garp all 命令显示所有设置的结果。

Switch#**show garp port** 10

Port	PortStatus	JoinTime(ms)	LeaveTime(ms)	LeaveAllTime(ms)
10	disable	200	100	1200

Switch#

5.3.16.2 设置静态组播组

用户执行该命令配置静态组播组。

【命令格式】set multicast vid <1-4094> mac-addr <HH:HH:HH:HH:HH:HH>

eport<portlist> Egress port list

fport<portlist> Forbidden egress port list

status <invalid/permanent> The static multicast group status

【使用指南】vlan、mac-addr 项是必须的，然后可以选择设置 eport、fport 或者 status。其中 status 只有在组播组存在的情况下才能够设置生效。把状态设置为 invalid 相当于删除多播设置。

【参数说明】<1-4094>是 Vlan Id，标识所在的 vlan；<HH:HH:HH:HH:HH:HH>为组播 mac 地址；如果选择设置 eport，<portlist>为发送组播报文端口号；如果选择设置 fport，<portlist>为禁止组播报文发送的端口号；如果选择设置 staus 为静态组播组的属性，支持下列 2 种属性类型：invalid，permanent

【举例】

Switch#**set multicast vid** 1 **mac-addr** 01:00:5e:e2:05:02 **eport** 2

Successfully set static multicast to egress port.

Switch#

Switch#**set multicast vid** 1 **mac-addr** 01:00:5e:e2:05:02 **fport** 5

Successfully set static multicast to forbidden port.

Switch#

Switch#**set multicast vid** 1 **mac-addr** 01:00:5e:e2:05:02 **status** permanent

Successfully set static multicast status.

Switch#

可以用下面的命令显示设置的结果。

Switch#**show multicast**

VlanId	MacAddress	EgressPort	Forbidden	Port Status
1	01:00:5e:e2:05:02	2	5	permanent

Switch#

5.3.16.3 gvrp命令

“ gvrp ” 命令集完成对 GVRP 协议的使能和禁止功能。

禁止 gvrp 协议

该命令禁止 GVRP 协议。

【命令格式】set gvrp disable

【参数说明】无任何参数

【举例】

Switch#**set gvrp disable**

Successfully disable GVRP protocol.

Switch#

使能 gvrp 协议

该命令使能 GVRP 协议。

【命令格式】set gvrp enable

【参数说明】无任何参数

【举例】

Switch#**set gvrp enable**
Successfully enable GVRP protocol.
Switch#

基于端口的 gvrp

该命令用于设置指定端口的 GVRP 协议属性。

设置接收报文的类型

该命令设置端口的 gvrp 协议可以接收的报文类型。

【命令格式】set port <portlist|all>gvrp acceptableframe <all|tag>

【参数说明】<portlist|all>为交换机物理端口列表，输入的形式可以是“ 1－2 ”或者“ 1，2，4－6 ”，如果要设置全部的物理端口可以使用 “ all ” 参数项；<all|tag>为可接收的报文类型，目前支持两种类型：all，tag，最好用“ ”括起来。

【举例】

Switch#**set port** 5-8 **gvrp acceptableframe tag**
Successfully set gvrp port acceptable frame type.
Switch#

禁止端口的 gvrp

该命令禁止指定端口的 gvrp 功能。

【命令格式】set port <portlist|all>gvrp disable

【参数说明】<portlist|all>为交换机物理端口列表，输入的形式可以是“ 1－2 ”或者“ 1，2，4－6 ”，如果要设置全部的物理端口可以使用 “ all ” 参数项。

【举例】

Switch#**set port** 5-8 **gvrp disable**

Successfully forbidden ports' gvrp protocol.

Switch#

使能端口的 gvrp

该命令使能指定端口的 gvrp 功能。

【命令格式】set port <portlist|all>gvrp enable

【参数说明】<portlist|all>为交换机物理端口列表，输入的形式可以是“ 1－2 ”或者“ 1，2，4－6 ”，如果要设置全部的物理端口可以使用 “ all ” 参数项。

【举例】

Switch#**set port** 5-8 **gvrp enable**

Successfully enable ports' gvrp protocol.

Switch#

使能端口的 ingressfilter

该命令设置使能端口的 ingress filter 状态。

【命令格式】set port <portlist|all>gvrp ingressfilter enable

【参数说明】<portlist|all>为交换机物理端口列表，输入的形式可以是“ 1－2 ”或者“ 1，2，4－6 ”，如果要设置全部的物理端口可以使用 “ all ” 参数项；

【举例】

Switch＃**set port** 5-8 **gvrp ingressfilter enable**

Successfully enable gvrp ports’ ingress filter.

Switch＃

禁止端口的 ingressfilter

该命令设置使能端口的 ingress filter 状态。

【命令格式】set port <portlist|all>gvrp ingressfilter disable

【参数说明】<portlist|all>为交换机物理端口列表，输入的形式可以是“1－2”或者“1，2，4－6”，如果要设置全部的物理端口可以使用“all”参数项；

【举例】

Switch#**set port** 5-8 **gvrp ingressfilter disable**

Successfully disable gvrp ports' ingress filter.

Switch#

pvid 命令

该命令设置指定端口 pvid。

【命令格式】set port <portlist|all> gvrp pvid <1-4094>

【参数说明】<portlist|all>为交换机物理端口列表，输入的形式可以是“1－2”或者“1，2，4－6”，如果要设置全部的物理端口可以使用“all”参数项；<1-4094>为端口的 Vlan 标识 PVID,该参数为可选，默认情况下，端口的 vlan 标识为 1。

注意：

1. **vlan 标识必须是一个已经存在的 vlan 标识。如果命令行中使用的 vlan 标识不存在，设置**

就会不成功。

2. **选择的端口列表中全部的端口必须处于同一个 vlan 中，否则设置不成功。**

【举例】

Switch＃**set port** 5-8 **gvrp pvid** 2

Successfully set ports' vlan id.

Switch＃

可以用下面的命令显示 gvrp 设置的结果。

Switch#**show gvrp port**

Port	PortId	Acceptable Type	Filter	Status	Fail Regist	Last GVRP Pdu
1	1	admitAll	disable	enable	0	00:00:00:00:80:3f
2	1	admitAll	disable	enable	0	00:00:00:00:80:3f
3	1	admitAll	disable	enable	0	00:00:00:00:80:3f
4	1	admitAll	disable	enable	0	00:00:00:00:80:3f
5	2	admitTag	disable	disable	0	00:00:00:00:80:3f
6	2	admitTag	disable	disable	0	00:00:00:00:80:3f
7	2	admitTag	disable	disable	0	00:00:00:00:80:3f
8	2	admitTag	disable	disable	0	00:00:00:00:80:3f

Switch#

5.3.17 端口聚合管理

5.3.17.1 lacp协议

禁止 lacp 协议

该命令禁止 LACP 协议。

【命令格式】set trunk lacp disable

【参数说明】无任何参数

【举例】

Switch#**set trunk lacp disable**

Successfully disable lacp protocol.

Switch#

使能 lacp 协议

该命令允许 LACP 协议。

【命令格式】set trunk lacp enable

【参数说明】无任何参数

【举例】

Switch#**set trunk lacp enable**

Successfully enable lacp protocol.

Switch#

设置关键号

用户执行该命令设置端口的 adminkey（关键号）。

【命令格式】set trunk lacp port <1-8> adminkey <1-32>

【参数说明】<1-8>为要聚合的物理端口号，取值为 1-8；<1-32>为 1-32 的整形数值；

【举例】

Switch#**set trunk lacp port** 2 **adminkey** 5

Port(s) 2 are assigned to admin key 5.

Switch#

用户可以通过 show trunk lacp 查看配置。

switch#show trunk lacp

Port	LACP	Key	Aggregator
1	enable	1	1
2	enable	5	2
3	enable	1	3
4	enable	1	4
5	enable	1	5
6	enable	1	6
7	enable	1	7
8	enable	1	8

switch#

使能端口聚合

用户执行该命令使能端口聚合。

【命令格式】set trunk lacp port <1-8> enable

【参数说明】<1-8>为要聚合的物理端口号，取值为 1-8；

【举例】

Switch#**set trunk lacp port** 2 **enable**

Successfully enable ports' LACP.

Switch#

关闭端口聚合

用户执行该命令关闭端口聚合。

【命令格式】set trunk lacp port <1-8> disable

【参数说明】<1-8>为要聚合的物理端口号，取值为 1-8；

【举例】

Switch#**set trunk lacp port** 3 **disable**

Successfully disable ports' LACP.

Switch#

用户可以通过 show trunk lacp 查看设置结果

Switch#**show trunk lacp**

Port	LACP	Key	Aggregator
1	enable	1	1
2	enable	1	2
3	disable	1	3
4	enable	1	4
5	enable	1	5

6	enable	1	6
7	enable	1	7
8	enable	1	8

Switch#

设置负荷分担算法

用户执行该命令设置端口采用何种聚合负荷分担算法。

【命令格式】set trunk lacp port <1-8> rules

<srcMAC|destMAC|srcXORDestMAC|srcIP|destIP|srcXORDestIP>

【参数说明】<1-8>为要聚合的物理端口号，取值为 1-8；

<srcMAC|destMAC|srcXORDestMAC|srcIP|destIP|srcXORDestIP>为负荷分担算法类型，支持下列方式：

srcMAC

destMAC

srcXORDestMAC

srcIP

destIP

srcXORDestIP

【举例】

Switch#**set trunk lacp port** 2 **rules** destMAC

Successfully link aggregator load share policy.

Switch#

5.3.17.2 静态聚合

该命令集下的子命令完成对静态端口聚合设置。

禁止静态端口聚合

该命令禁止指定的端口具有静态端口聚合。

【命令格式】set trunk static port <1-8> down

【参数说明】<1-8>为要聚合的物理端口号。

【举例】

Switch#**set trunk static port** 2 **down**

Successfully disable port static trunk.

Switch#

可以用下面的命令显示 static 设置的结果

Switch#**show trunk static**

Port	Status	Aggregator
1	up	1
2	down	2
3	up	3
4	up	4
5	up	5
6	up	6
7	up	7
8	up	8

Switch#

使能静态端口聚合

该命令允许指定的端口具有静态端口聚合。

【命令格式】set trunk static port <1-8> up

【参数说明】<1-8>为要聚合的物理端口号。

【举例】

Switch#**set trunk static port** 2 **up**

Successfully set port static trunk up.

Switch#

设置静态端口聚合

该命令设置静态端口聚合

【命令格式】1.set trunk static port <1-8> to <1-8>

2.no set trunk static port <1-8>

【参数说明】命令 1port 后面的<1-8>为要聚合的物理端口号；to 后面的<1-8>为要聚合到的端口号。命令 2 是取消对端口聚合的设置

注意：

1. **设置静态聚合时应先关闭 LACP 协议**
2. **在设置静态端口聚合时，aggregator 的端口号应小于 aggregation 的端口号**
3. **取消对端口聚合设置时输入参数为 aggregation 端口号**

【举例】

Switch#**set trunk static port** 2 **to** 1

bind port 2 to port 1 .

Switch#

Switch#**no set trunk static port** 2

Successfully clear the aggregation.

Switch#

可以用下面的命令显示 aggregater 设置的结果

Switch#show trunk aggregator

	1	2	3	4	5	6	7	8
1	M	M	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-
3	-	-	M	-	-	-	-	-
4	-	-	-	M	-	-	-	-
5	-	-	-	-	M	-	-	-
6	-	-	-	-	-	M	-	-
7	-	-	-	-	-	-	M	-
8	-	-	-	-	-	-	-	M

Switch#

第六章 WEB管理

交换机还提供了一个内置的基于 WEB 方式的网络管理系统，用户可以位于网络的任何地方通过标准的浏览器（Microsoft Internal Explorer 4.x 及以上）来管理交换机，由于浏览器的版本不同，你看到的访问界面可能与下文中的图示不太相同。

6.1 准备工作

首先，需要在你的计算机上安装好浏览器软件（Microsoft Internal Explorer 4.x 及以上），安装方法详见浏览器自己的安装说明。

其次，需要配置交换机的 IP 地址，可以在控制台界面中手动设置。见 5.2.2 配置交换机 IP 地址。

6.2 WEB管理界面配置说明

运行浏览器，在浏览器的 URL 地址栏中输入交换机的 IP 地址，就可以通过 WEB 访问交换机。假设交换机的 IP 地址为：192.168.32.139，则在 URL 中输入 http://192.168.32.139，然后点击 Enter 键，即可进入 WEB 管理界面。

初次进入视窗管理界面，会出现用户名和密码对话框。输入登录名“ admin ”，密码“ password”，即可进入管理主画面，并可看见设备的前面板图标。

所有可操作菜单皆罗列于视窗的左侧，用户可通过直接点击相应功能项，进入下层菜单。

绝大多数设置画面都具有接受设置 **apply** 及 **save** 选项。“ 接受设置 ”表示修改参数并刷新界面，“ save ”表示存储参数。

对于页面正上方的交换机面版图是动态更新的，用户可以通过点击端口的 Link 灯查看端口状态。

注意：点击 apply 只对当前设置生效，如需将设置存储于 NVRAM，则需 save 功能使之生效。

初次进入视窗管理界面时的界面如下图所示：

该页面显示交换机的基本配置信息：包括交换机的设备类型描述，交换机的 MAC 地址（不可改变），IP 地址，子网掩码，缺省网关 IP 地址，交换机的位置描述及其它二、三层协议的使能、禁止开关。以后会详细介绍该各项配置。

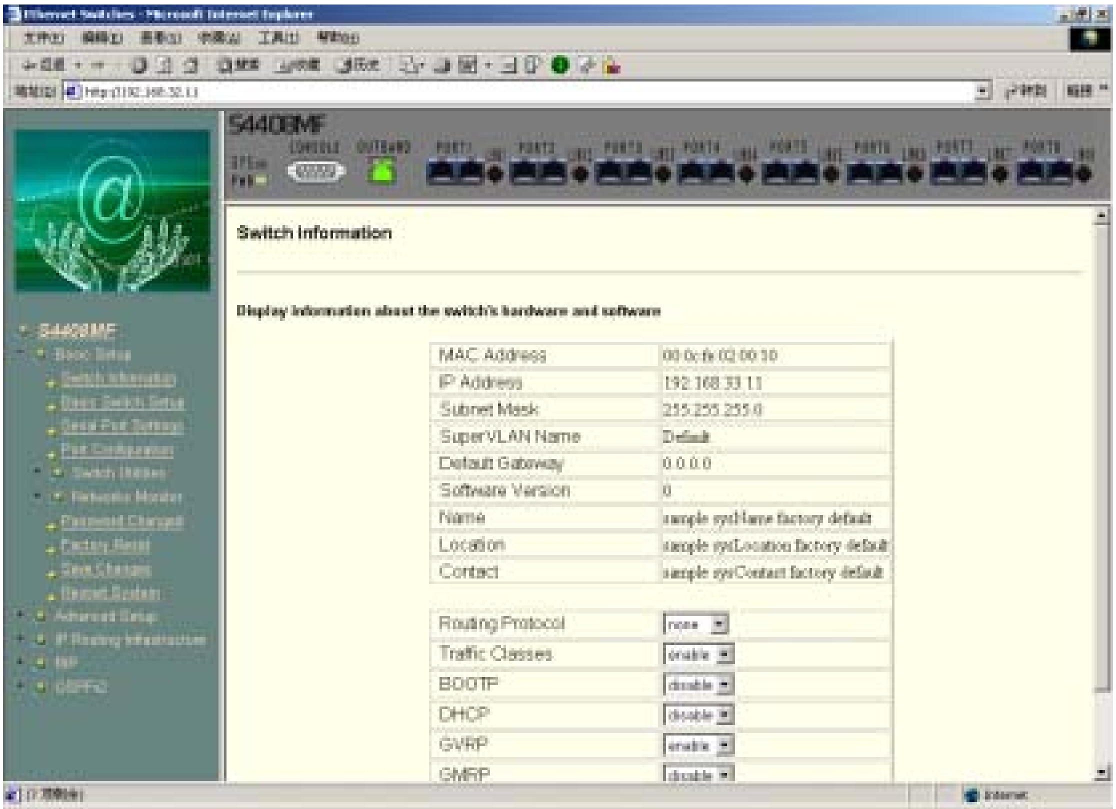


图 6－1 WEB 管理初始界面

6.2.1 基本配置

展开左侧的“ Base Setup ”，会下拉出配置信息的各个表项，点击相应的表项，即可对相应信息进行配置或产生相应操作。

6.2.1.1 交换机信息（Switch Information）

点击配置页面左侧的“ Switch Information ”，会打开图 6-1 所示的初始界面，显示该交换机的基本配置信息。

6.2.1.2 交换机基本信息配置(Basic Switch Setup)

点击配置页面左侧的“ Basic Switch Setup ”，打开图 6-2 所示的配置界面，显示目前的配置信息及可以对该交换机进行新的配置的文本框。内容包括：

IP address：交换机的 IP 地址

SubNetMask：交换机的子网掩码

Default Gateway：缺省网关的 IP 地址

VLAN Name：缺省 VLAN1 的名称

Routing Protocol：路由协议的使能，包括：none，rip，ospf

IGMP Snooping：该协议的使能禁止开关

Link Aggregation：链路聚合的使能禁止开关

STP：STP 协议的使能禁止开关

Name：用户指定的交换机名，对应于 SNMP MIB II 中的 system.sysName 变量；

Location：用户定义的交换机所在的位置描述，对应于 SNMP MIB II 中 system.sysLocation 变

量；

Contact：系统维护的联系人，对应于 SNMP MIB II 中的 sysContact 变量。

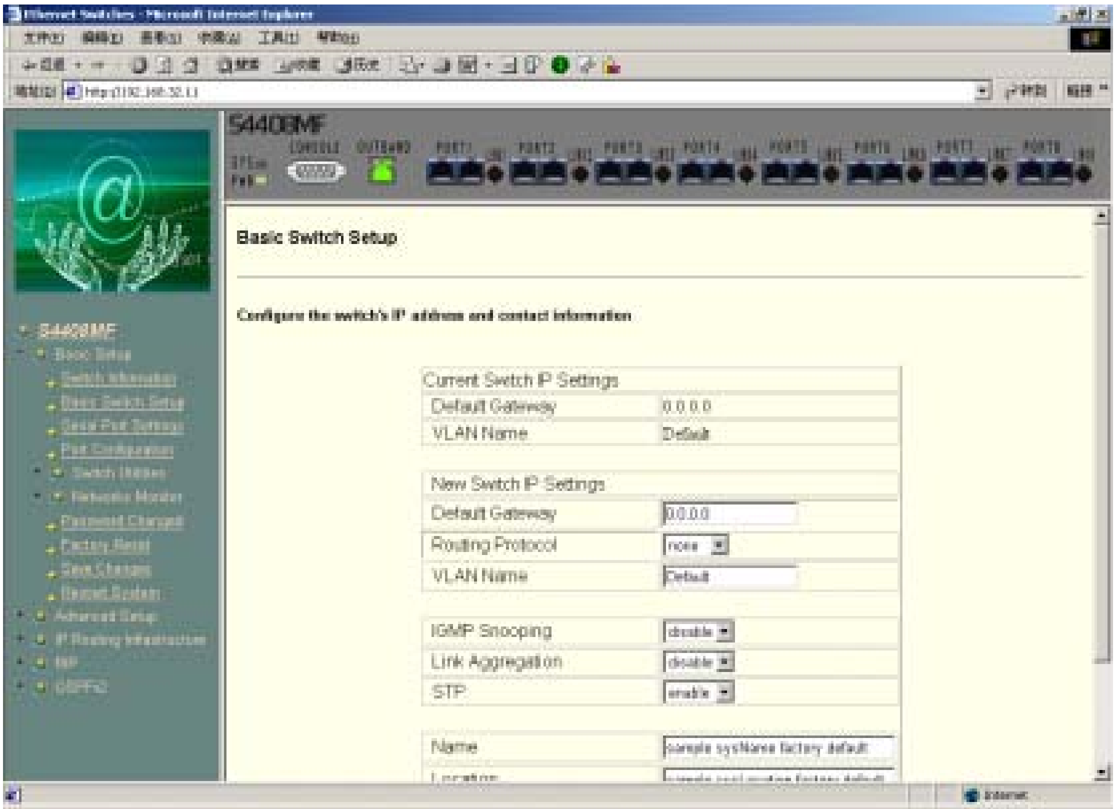


图 6－2 Basic Switch Setup 界面

6.2.1.3 配置串口属性(Serial Port Setting)

点击配置页面左侧的“ Serial Port Setting ”，会打开图 6-3 所示的串口属性配置界面，本页面完成对串口属性的配置，包括波特率、数据位、奇偶校验、停止位等属性。

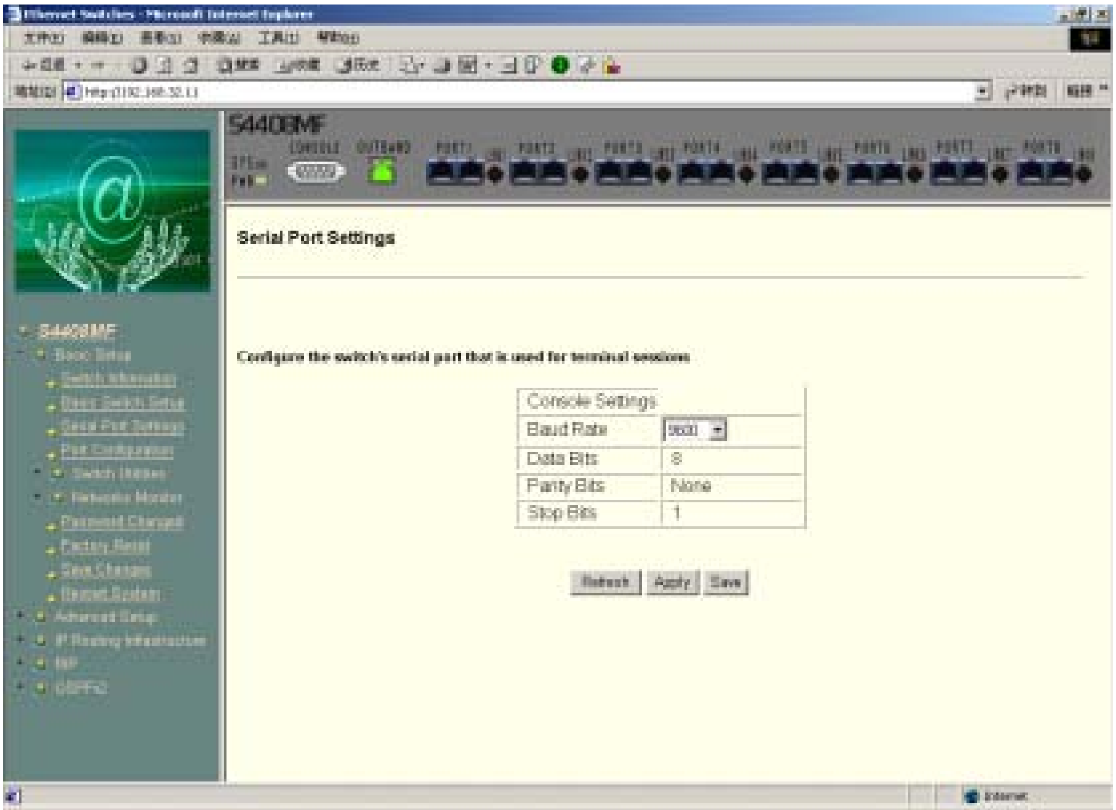


图 6－3 Serial Port Setting 界面

6.2.1.4 端口配置（Port Configuration）

点击配置页面左侧的“ Port Configuration ”，会进入图 6-4 所示的端口信息显示界面，该界面列出了全部 8 个端口的状态、连接状态及端口速率等信息。选择某个端口后点击“ Edit ”按钮会弹出图 6-5 所示的对话框，利用该对话框可以对该端口进行设置了，可按如下步骤进行：

1. 在“ State ”中，Enable 或 Disable 该端口，如果拥护选择“ Disable ”，那么连接在该端口的设

备将不能使用交换机，并且在 MAC 地址表老化后，交换机会将该设备的 MAC 地址从地址表中清除掉。但是，如果该设备的 MAC 地址在静态地址表中，则不会被老化清除。

2. 对话框中还可以看出该端口的实际速率、类型、STP 状态等。

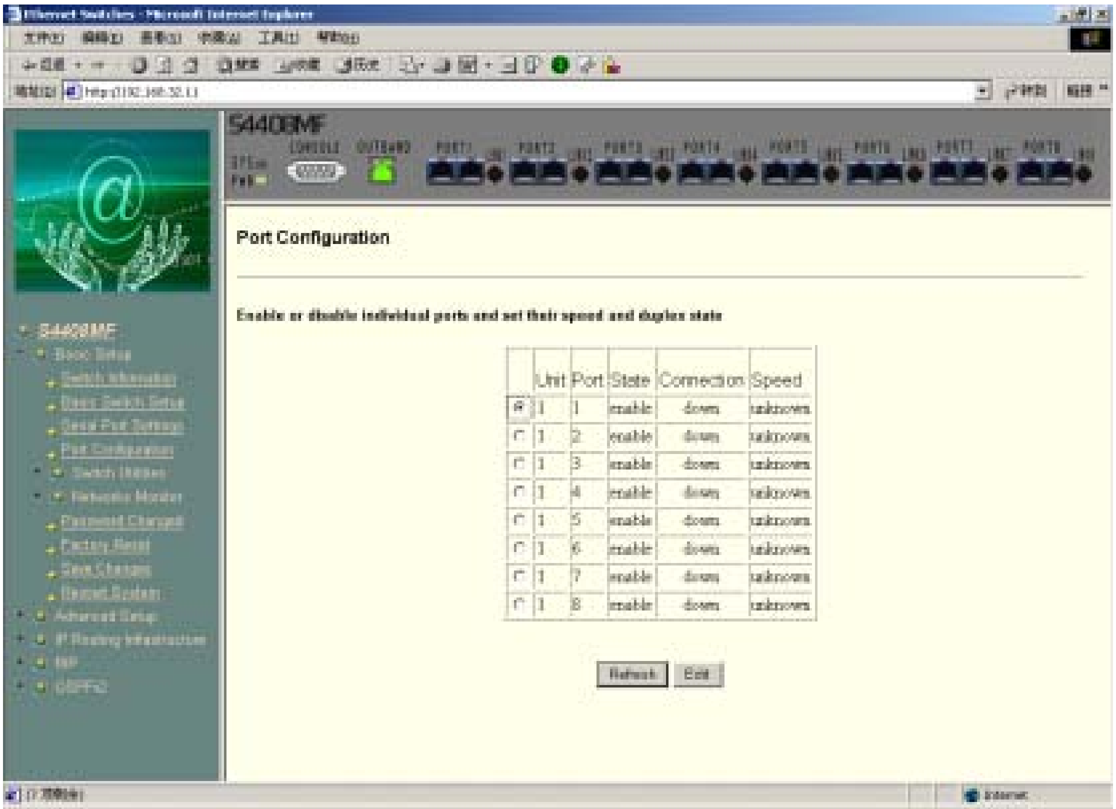


图 6－4 端口信息

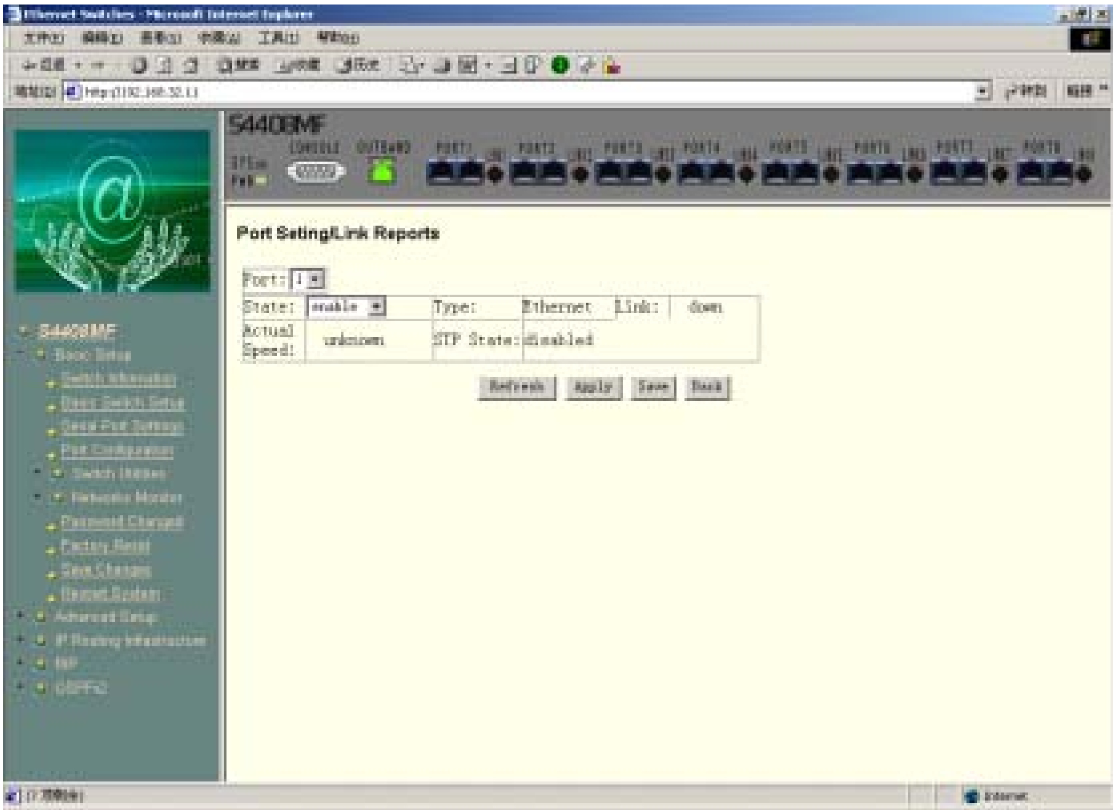


图 6－5 端口配置

6.2.1.5 工具配置（Switch Utilities）

点击配置页面左侧的“ Switch Utilities ”,并按图 6-6 配置页面左侧展开,点击第一个“ Download Software ”， 会显示如图所示配置页面。

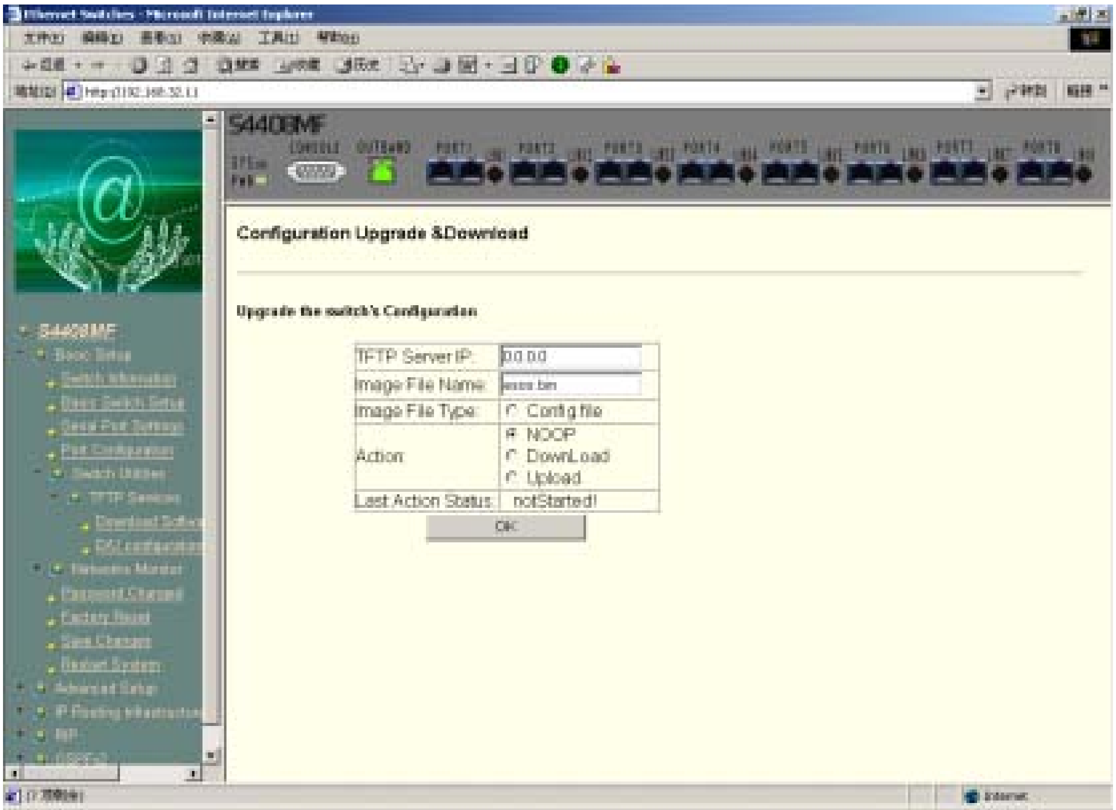


图 6－6 Software Download

界面中各项的含义说明如下：

- TFTP Server IP：软件所在的 TFTP 服务器的 IP 地址；
- image File Name：TFTP 服务器上的镜像文件所在的路径和文件名；
- image File Type：上传或下载的镜像文件类型， 包括两种类型：应用文件和配置文件；
- action：软件升级的动作，支持三种操作：不动作、download；

♦ Last action status：最后一个动作完成后的结果，无论成功与否。

点击第二个“ D/U ”，除了 **image File Type** 有所变动外，其它操作同图 6-6 所示完全相同。

6.2.1.6 网络监视信息（Networks Monitor）

点击配置页面左侧的“ Networks Monitor ”路径下的“ Statistics ”，会看到端口的统计信息列表。

端口利用率（Port Utilization）

点击“ Port Utilization ”，会进入如图 6-7 所示界面。

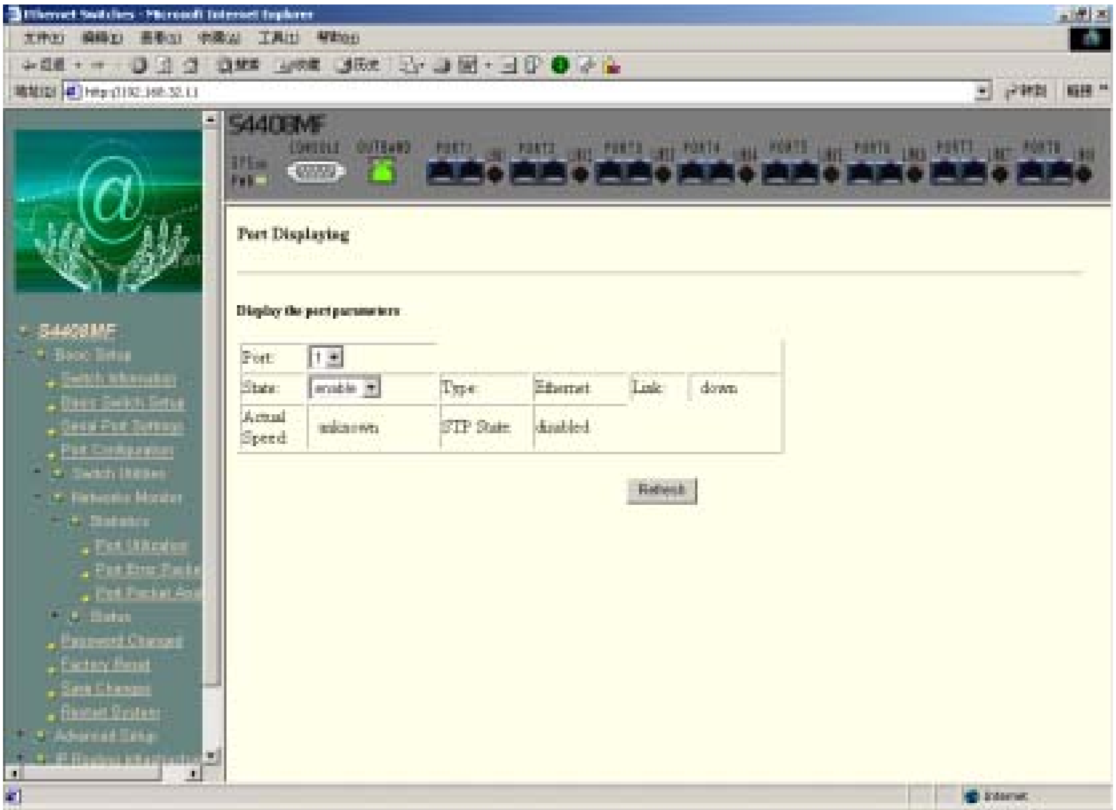


图 6－7 Port Utiization

该界面同 6-5 的界面的部分功能相同，但只是显示各端口的配置，包括端口状态、端口速率及端口类型等。

端口错误包统计（Port Error Packets）

点击 " Port Error Packets "，会进入如图 6-8 所示界面。该界面显示了某端口所处理的出错数

据包的统计信息，包括：

Dropevents：自从最近一次交换机重启后，该端口丢弃帧的数量。

Jabbers：长度超过 1518 字节，同时出现 CRC 校验错误的数据包的数量。

Octes：长度小于 64 字节（所允许的最小字节数），却拥有正确的 CRC 的帧的数量。

Collisions：在该以太网段内发生的碰撞的估计总数。

Fragments：长度小于 64 字节的数据包的数量。

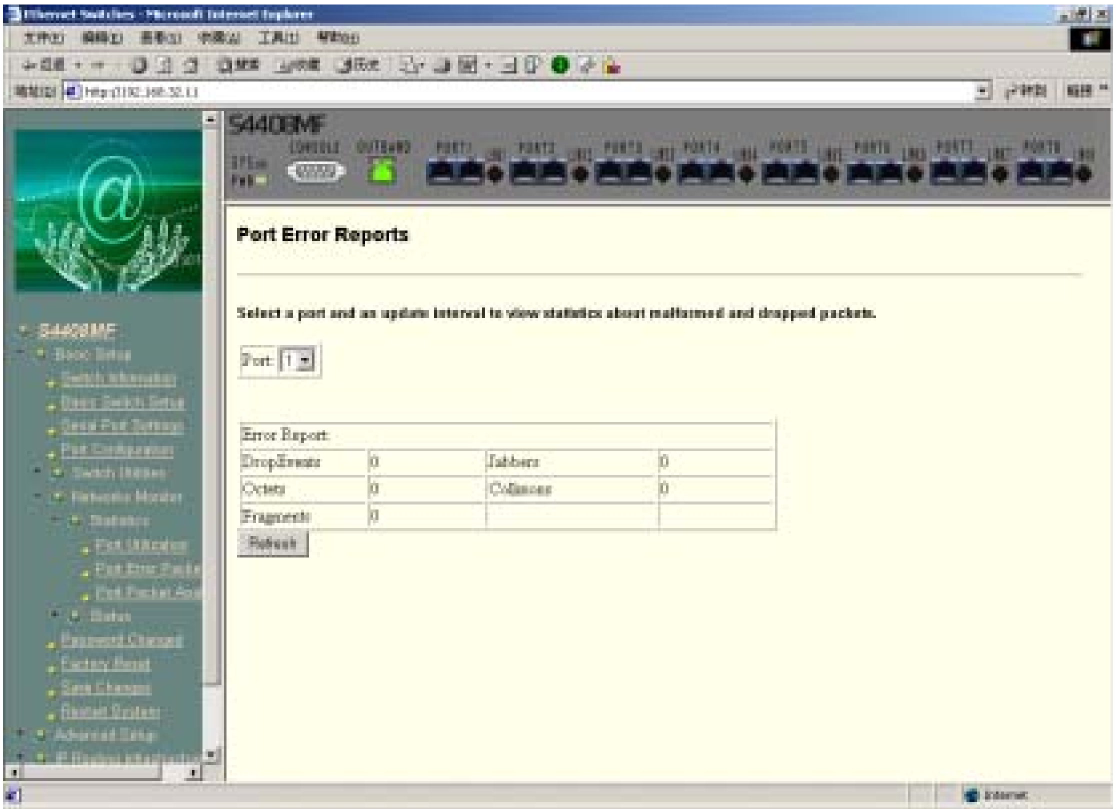


图 6－8 Port Error Packets

端口数据包分析（Port Packet Analysis）

界面中各项数据分析如图 6-9 所示，各项的含义说明如下：

Pkts：该端口接收到的数据包的总量，包括正常的和异常的。

Pkts64Octets：该端口接收到的长度为 64 字节的数据包的总数，包括异常的数据包。

Pkts65-127Octets：该端口接收到的长度介于 65-127 之间的的数据包的总数，包括异常的数据包。

Pkts128-255Octets：该端口接收到的长度介于 128-255 之间的的数据包的总数，包括异常的数据包。

Pkts256-511Octets：该端口接收到的长度介于 256-511 之间的的数据包的总数，包括异常的数据包。

Pkts512-1023Octets：该端口接收到的长度介于 512-1023 之间的的数据包的总数，包括异常的数据包。

Pkts1024-1518Octets：该端口接收到的长度介于 1024-1518 之间的的数据包的总数，包括异常的数据包。

MulticastPkts：收到的和发送的正常的组播数据包的总数。

注意：不包括发送的广播地址的数据包。

BroadcastPkts：收到的和发送的正常的广播数据包的总数，注意：不包括发送的组播地址的数据包。

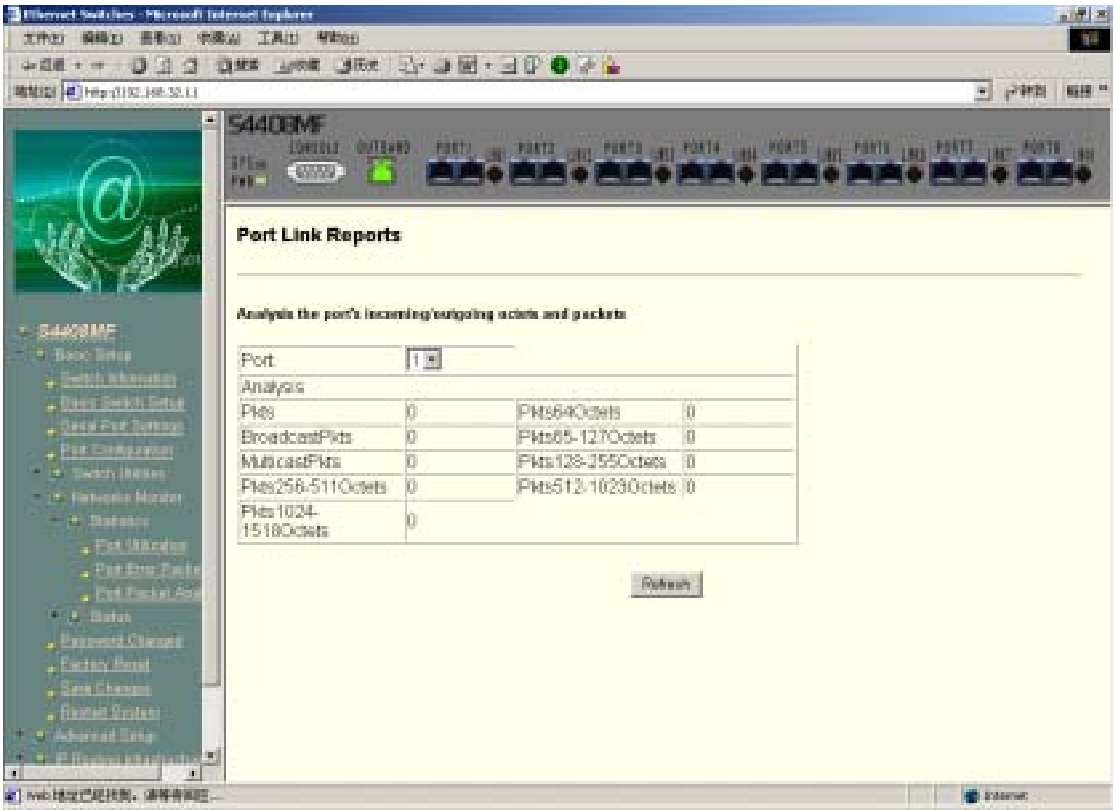


图 6－9 Port Packet Analysis

GVRP 状态（GVRP Status）

在配置页面左侧 “ Status ” 菜单下，点击 “ GVRP Status ”，进入 GVRP 状态表，该表显示了目前的 VLAN 配置，包括：

VID：VLAN 标识符；

Status：状态，静止态；

Create Time：创建时间，日－小时－分－秒；

Current Egress Ports：目前的输出端口，M 表示该端口为 VLAN 的成员；

Current Untagged Ports：目前的 Untagged 端口，U 表示该端口为 Untagged 端口。

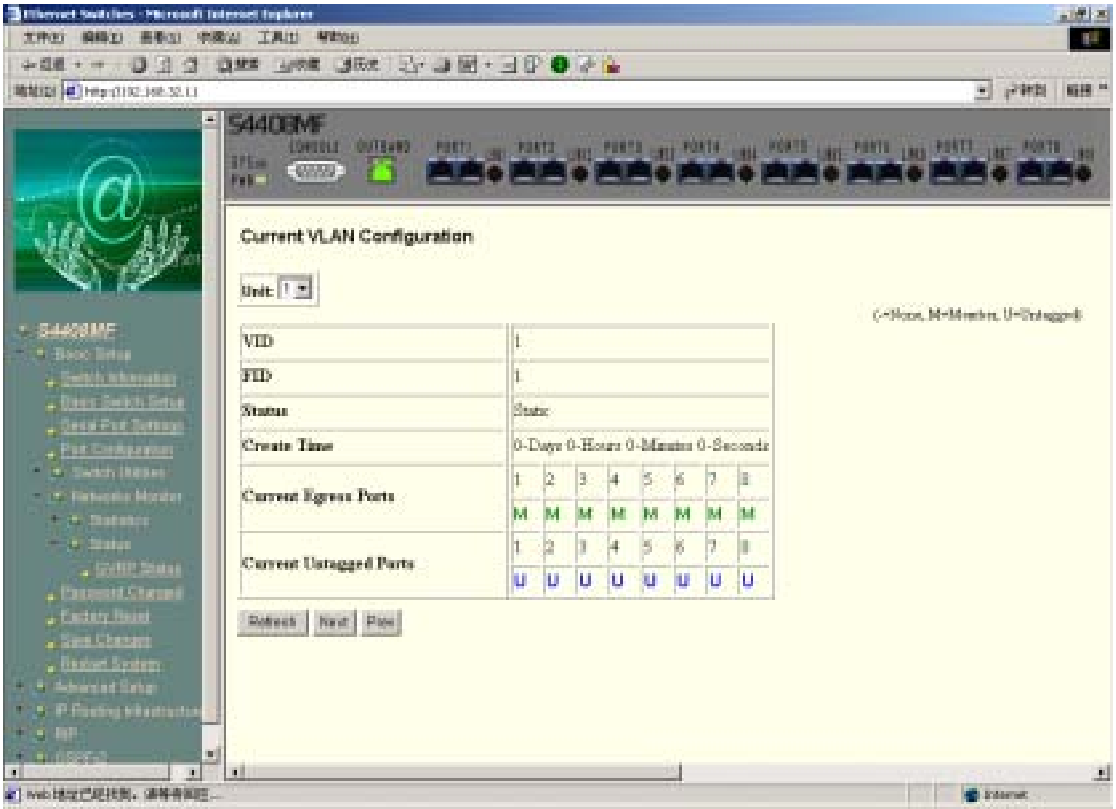


图 6-10 GVRP STATUS

6.2.1.7 恢复出厂设置（Factory Reset）

在页面左侧的主菜单，选择“ Factory Reset ”，将出现如下图所示界面：

在执行“ Factory Reset ”之前，请务必确定是否需要进行此操作。一旦执行了此操作，那么交换机所有存贮在 NV-RAM 内的设置（包括 TCP/IP 协议设置、SNMP 参数、端口上所有功能的设置、以及安全设置等）都将被删除，恢复为出厂时的缺省值。

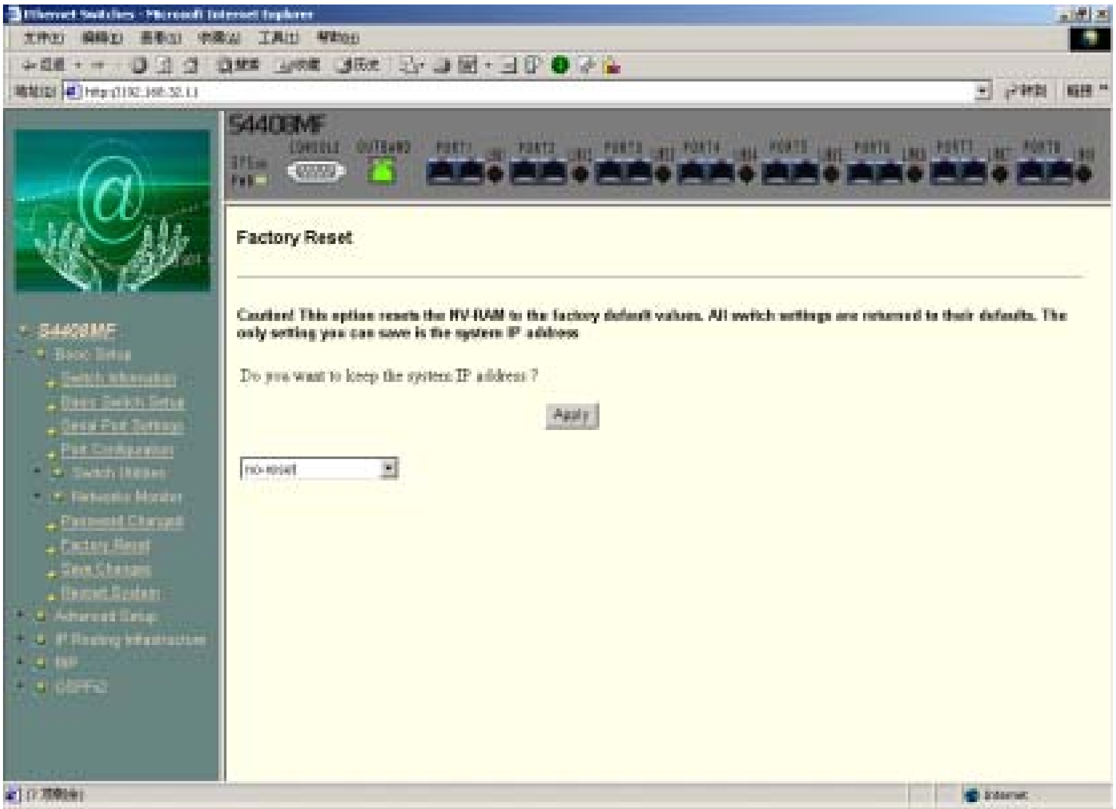


图 6－11 Factory Reset

6.2.1.8 存贮改变（Save Change）

在页面左侧的主菜单，选择“ Save Change ”，将出现如下图所示界面：

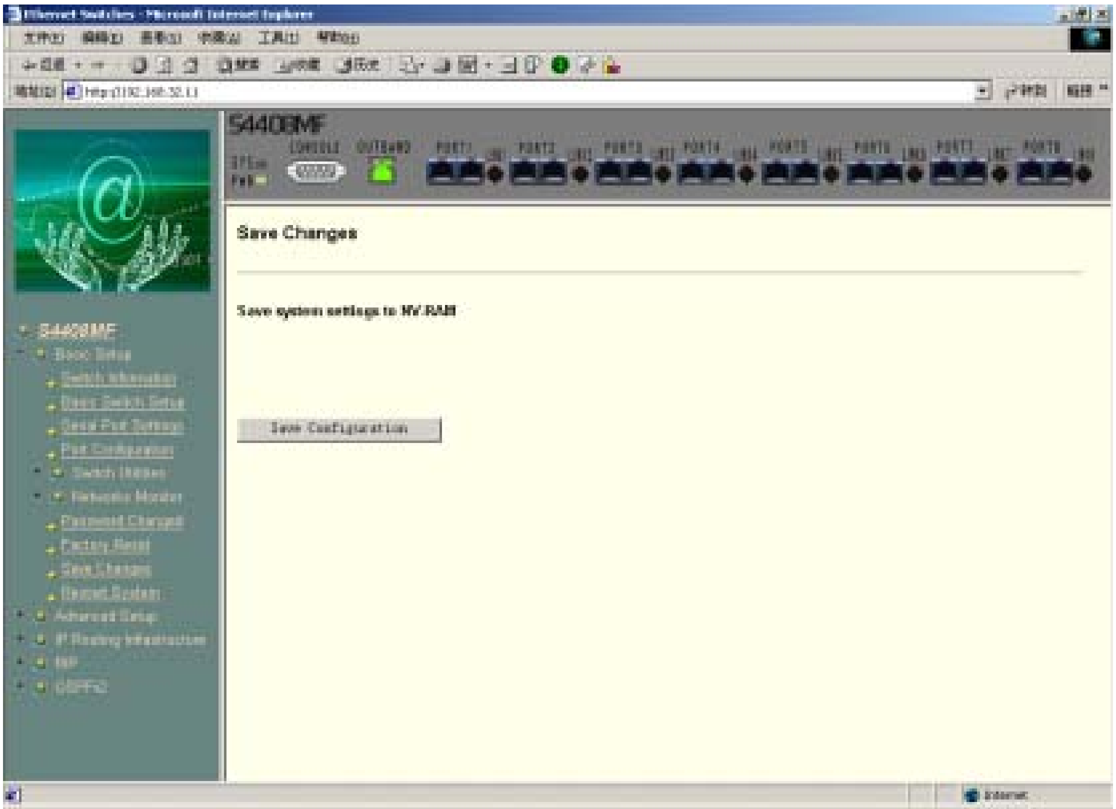


图 6-12 Save Changes

如果想将当前所有更改的设置值保存到交换机的闪存（flash memory），那么，按 Save Configuration 即可。一旦设置值存入 NV-RAM 中，它们将成为交换机的默认设置。

6.2.1.9 重启系统（Restart System）

在页面左侧的主菜单，选择“ Restart System ”,会弹出“ Restart ”按钮。如果想重启交换机，可以点击 Restart 按钮来实现热启动。

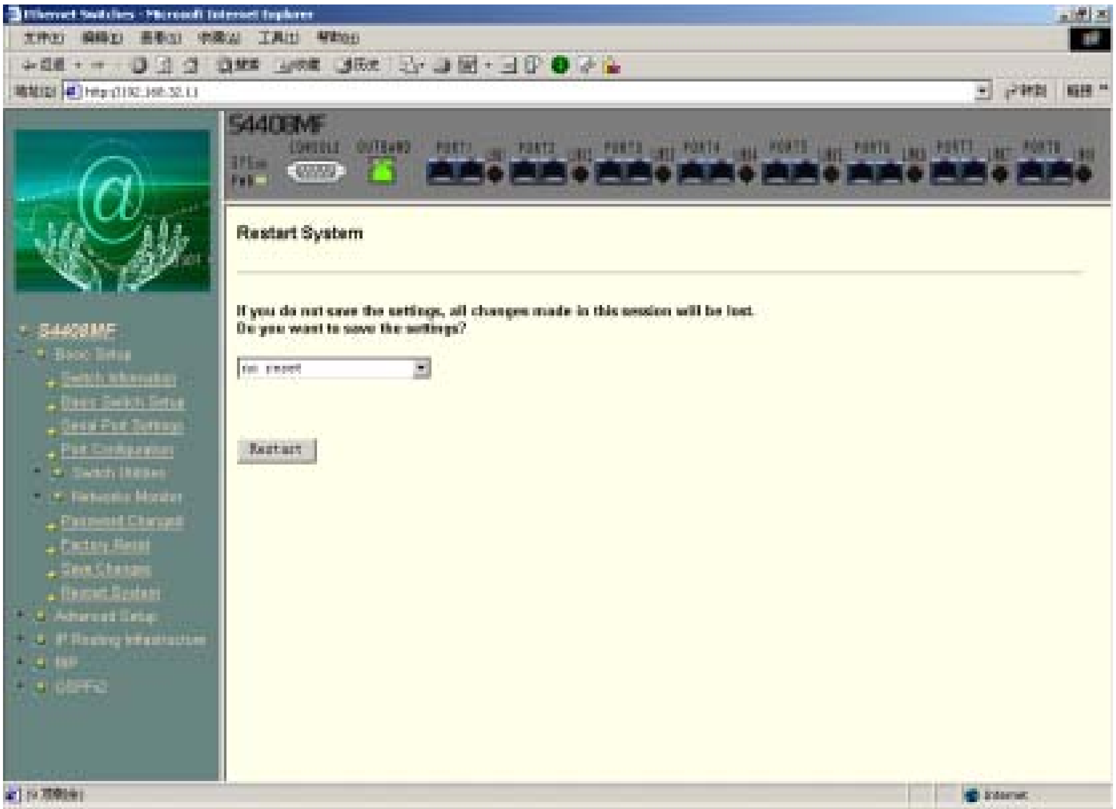


图 6-13 System Restart

6.2.2 高级配置（Advances Setup）

6.2.2.1 生成树配置（Spanning Tree）

S4408MF 交换机支持 IEE802.1D 生成树协议，允许用户创建备份路径，以保证网络的高可用连接性。有关生成树协议的详细内容，请参阅本手册的 4.7 节。

交换机生成树配置（STP Switch Settings）

如果想配置交换机的生成树功能，请在图 6－14 所示的各项中填入相应的参数，然后按 Apply 按钮。

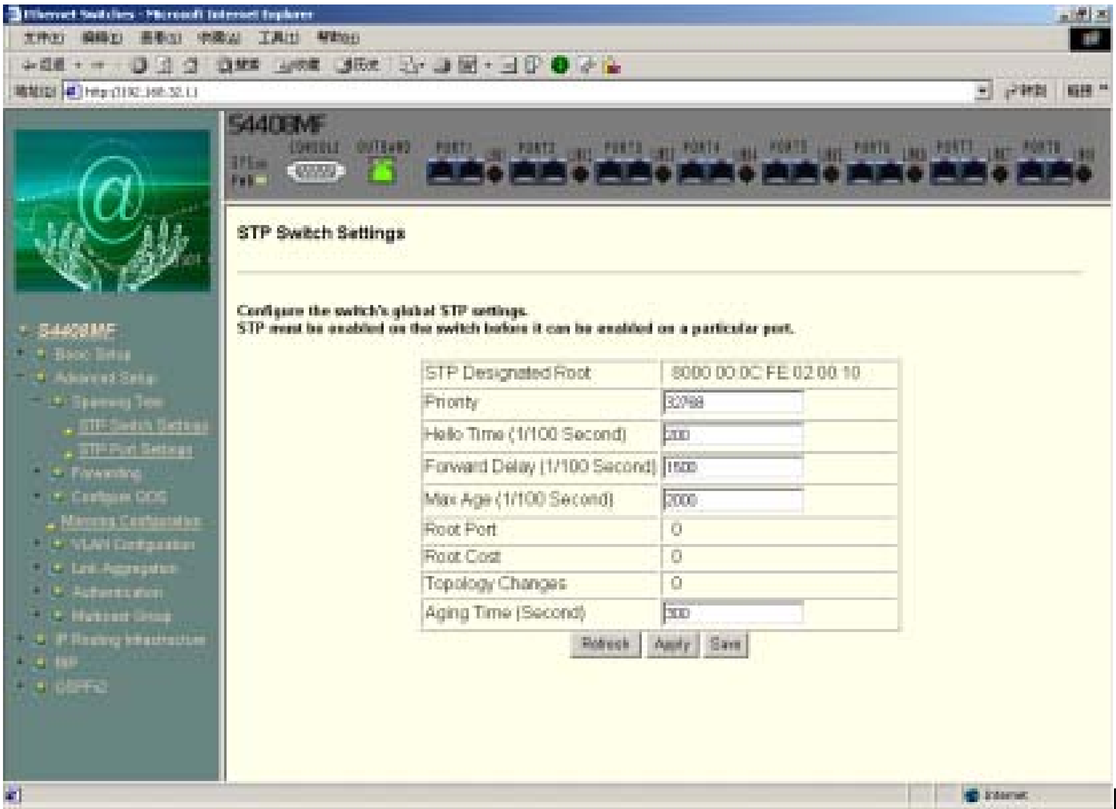


图 6－14 STP Switch Settings

界面中各项含义说明如下：

STP Designated Root：STP 指定的根桥的 MAC 地址；

Priority：为交换机设定的Priority，能设置成0 到65535 中的一个数值。0 代表最高优先权。这个数值将在网络交换机间的选举过程中使用来决定那一个交换机是根交换机。一个低交换机表明高优先权，并且这个交换机被选为根交换机的可能性也较高。

Hello Time：Hello Time 能被设置为从1 到10秒中的一个值。这是根网桥发送两个通知其它交换机它是根网桥的BPDU 包的发送时间间隔。如果你为你的交换机设置了一个Hello Time，并且它不是根网桥，设置Hello Time将在你的交换机成为根网桥时被使用。

注意：Hello Time 不能比Max. Age 长。另外，将要产生一个配置错误。

Forward Delay：Forward Delay 能设置成4 到30秒中的一个值。在从阻塞状态转换到转发状态时，这是任何交换机端口在侦听情况下所花费的时间。

Max Age：Max. Age 能被设置为从6 到40 秒中的一个值。在Max. Age 结束时，如果仍没有从根网桥接收到一个BPDU，你的交换机将开始发送它自己的BPDU 给其它所有交换机来确定成为根网桥。如果证实你的交换机有最低网桥标识符，它将成为根网桥。

注意：当设置上面的参数时，应遵守如下公式：

Max. Age ≤ 2 x (Forward Delay - 1 second)

Max. Age ≥ 2 x (Hello Time + 1 second)

Root Port：根端口，每台交换机都有一个根端口，这个端口到根桥的开销路径最低。

Root Cost：该交换机到根桥的路径开销。

Aging Time：MAC地址表的老化时间，老化时间的数值范围从10 秒~1,000,000 秒，缺省值为300秒。

注意：界面上所有值的配置单位为1/100秒。

端口生成树配置（STP Port Settings）

端口生成树配置界面如图 6-15 所示，在相应的窗口中输入欲设置的值，然后按 Apply。

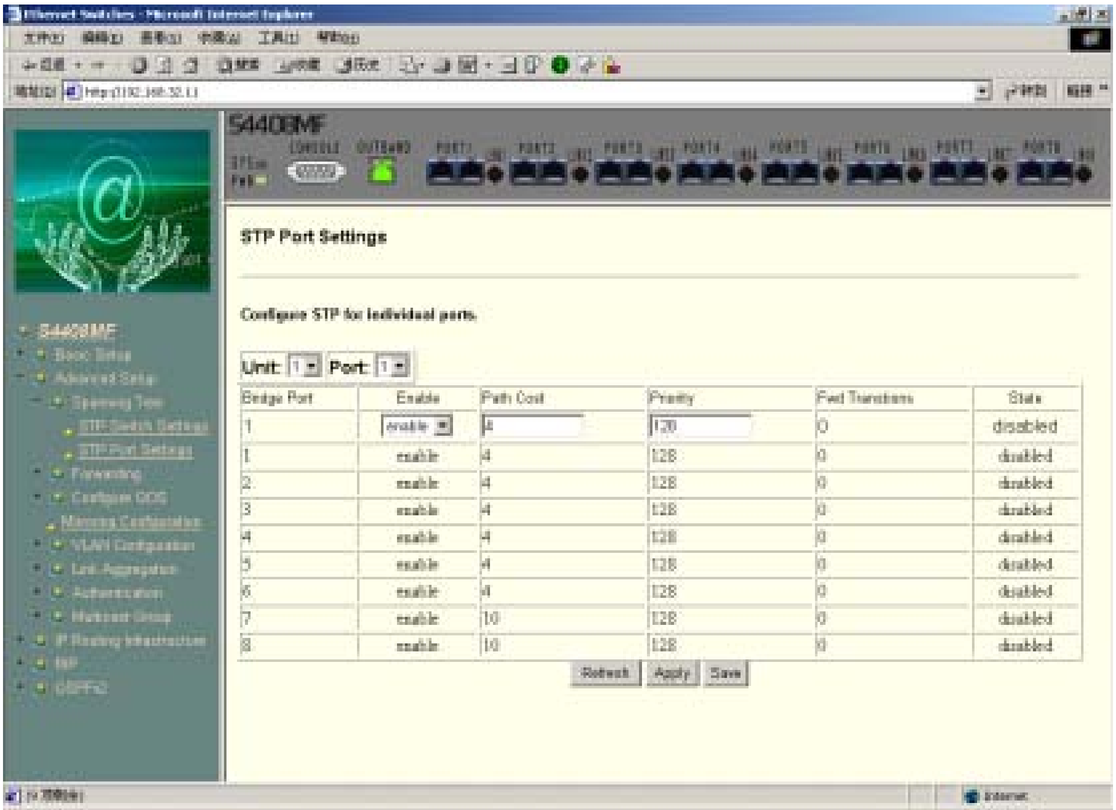


图 6－15 STP Port Settings

界面中各项含义说明如下：

Bridge Port：显示该交换机所有的物理端口号；

Enable：使能或禁止该端口的 STP 功能；

Path Cost：路径开销，它是一个可变的参数，可以根据生成树算法的指标进行修改。每个 1000Mbps 网段的路径开销值为 4。

Priority：口优先权可设置为从0 到255 中的一个数值。较小的数值表示端口有较大的可能性被选作为根端口。

Fwd Transitions：该端口从学习态到转发态的转变次数；

State：该端口的STP状态（阻塞、侦听、学习、转发态等）。

6.2.2.2 转发配置（Forwarding）

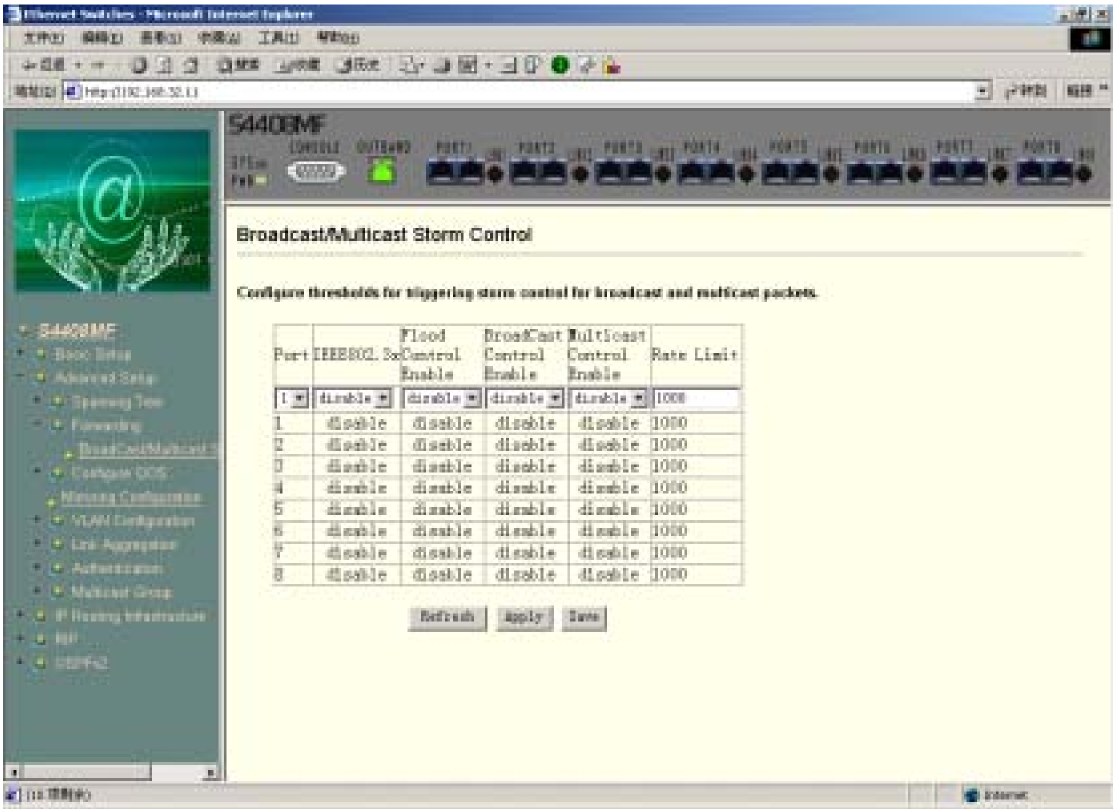


图 6-16 Broadcast/Multicast Storm Control

该配置界面用于广播/组播风暴控制，针对每个端口，都设置了控制广播/组播风暴的使能开关。

IEEE802.3x：IEEE802.3x 流量控制使能禁止开关；

Flood Control Enable：流量控制使能禁止开关；

BroadCast Control Enable：广播控制使能禁止开关；

Multicast Control Enable：组播控制使能禁止开关；

Rate Limit：对该端口的速率限制，单位为 packets/s。

6.2.2.3 QOS配置（Configure QOS）

在配置界面左侧的主菜单中点击“ QOS default priority ”，则进入基于端口的优先级配置界面。

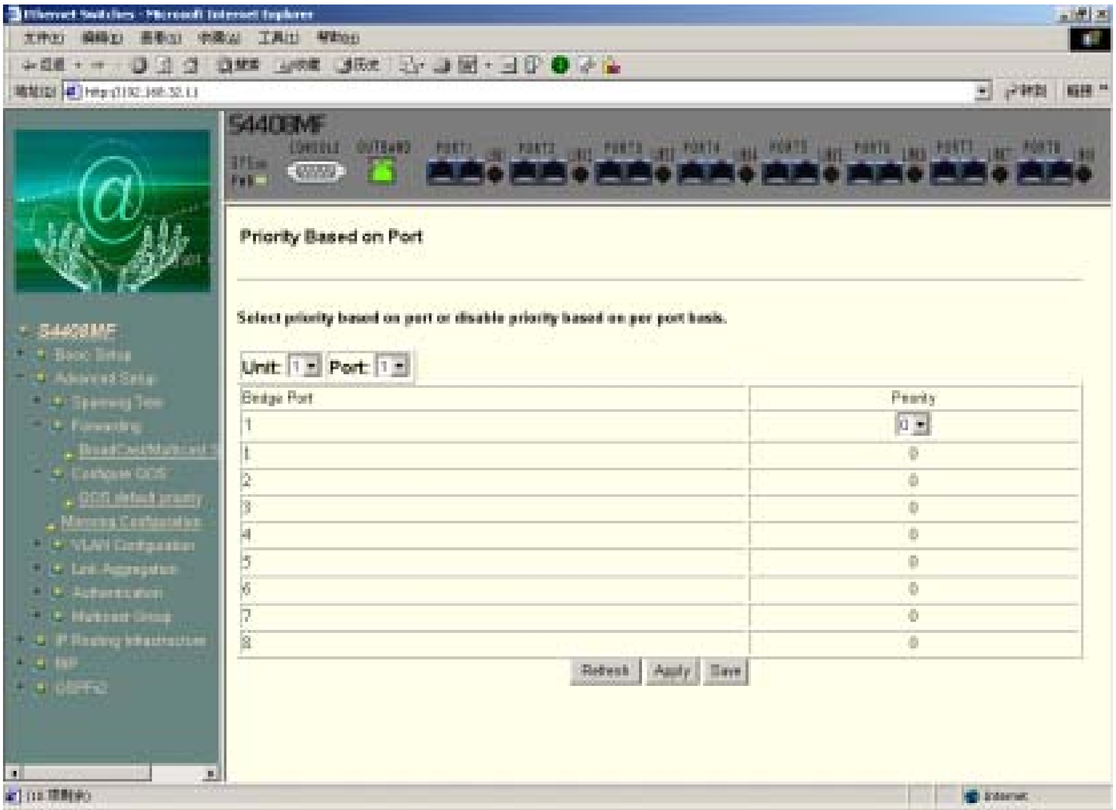


图 6-17 QOS default priority

该页面可以配置每个端口的 QoS 优先级，进而提供和识别 QoS 专用的包优先级。可以通过 2 层 VLAN 的优先标签来给数据包定义优先级别，并根据优先级进行数据包转发或丢弃，从而保证了服务质量。该优先级的设置遵循 802.1p 标准。

6.2.2.4 端口镜像配置（Mirroring Configuration）

S4408MF 交换机允许用户将某个或某几个端口收发的所有数据包复制一份到另外一个端口，

以便用户能够将一台监视设备（如 Sniffer 或 RMON Probe）连接到镜像端口上，来查看通过前一个或几个端口的所有数据包的详细情况。

选择配置界面左侧主菜单的“ Mirroring Configruation ”，将出现图 7-19 所示的界面。下面对各项分别进行介绍：

Switch Mirror Mode：为了实现端口镜像的功能，需要配置端口镜像模式“ Switch Mirror Mode ”，该模式提供三种选择：disable、L2、L2-L3。disable 表示禁止端口镜像功能，L2 表示只镜像二层数据包，L2-L3 表示二、三层数据包都可以进行镜像操作。

Mirror to Port Setting：用于选择镜像的目的端口，用户可以在该端口上连接监视或故障排除的设备，这样就可以监视源端口上发生的所有情况。

Port：用于选择镜像的源端口，该端口的数据包可以被复制到目的端口。

Interface Mirror Mode：提供源端口的镜像操作模式，该模式提供四种选择：none 、ingress 、egress、all。none 表示该端口不进行镜像操作；ingress 表示只对该端口的输入报文进行源端口镜像；egress 表示只对该端口的输出报文进行源端口镜像；all 表示对该端口的所有报文（包括输入和输出）进行源端口镜像。

注意：不能将一个高速端口镜像到一个低速端口上。例如，如果将一个 100Mbps 端口镜像到一个 10Mbps 端口，会造成吞吐量承受能力的问题。因此，源端口速率应和目的端口速率相同，或者更低，而且目的端口不能是端口干路（Trunk Group）的成员。

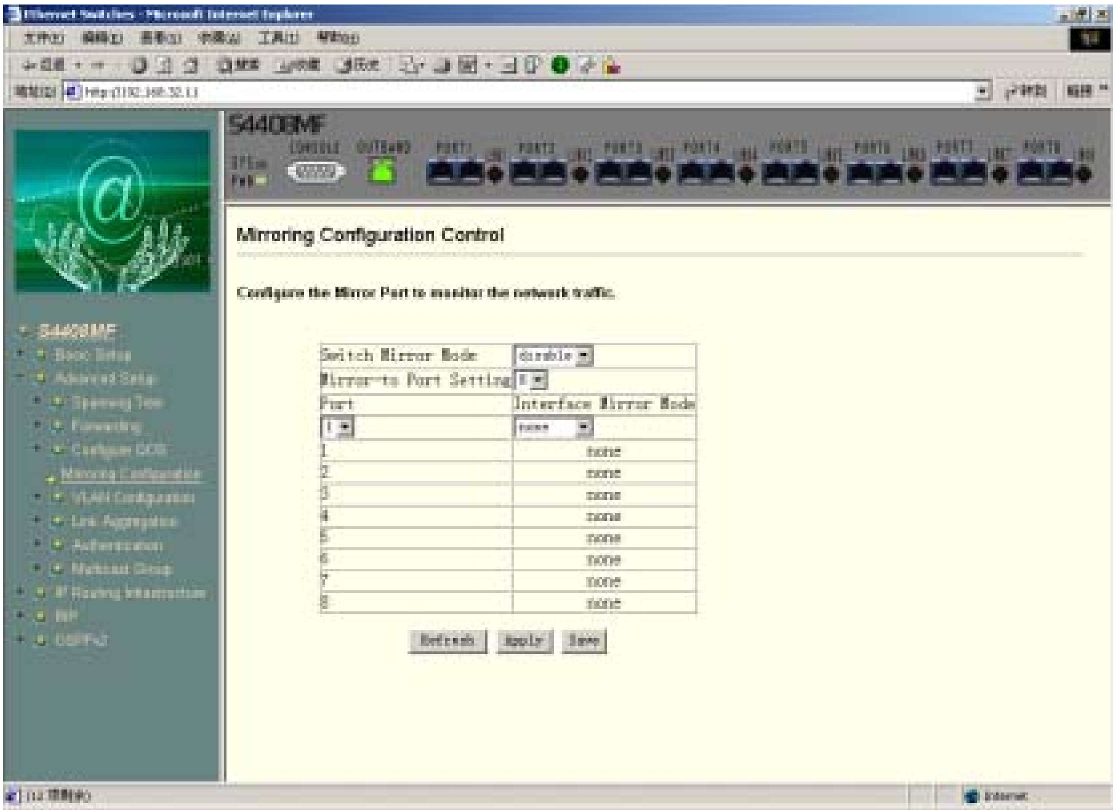


图 6－18 Mirroring configuration Control

6.2.2.5 VLAN配置（VLAN Configuration）

点击配置界面左侧主菜单中的“ VLAN Configuration ”，会下拉出三项配置。

GVRP 设置

交换机GVRP模式设置界面如图6－19所示，该页面只显示GVRP协议的使能开关，允许或禁止

VLAN 组注册协议允许成员动态加入VLAN中，点击Apply,使配置生效。

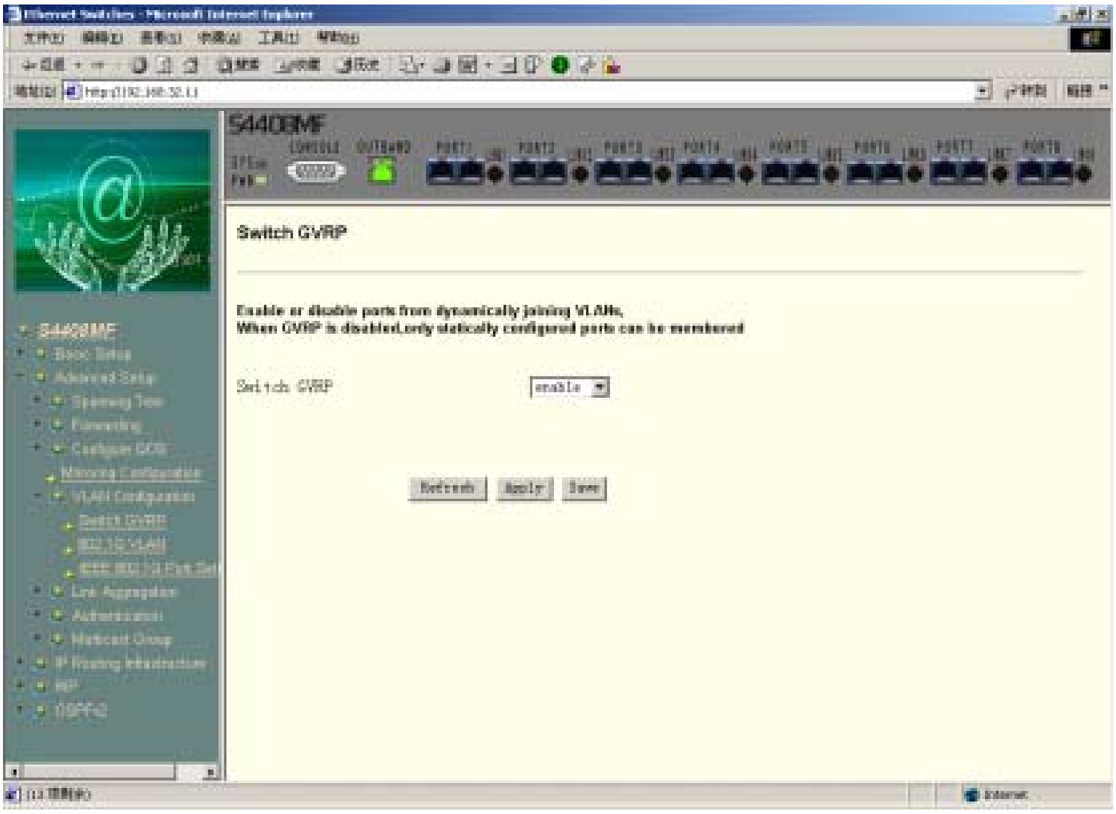


图 6-19 Switch GVRP

802.1Q VLAN 配置（802.1Q VLAN）

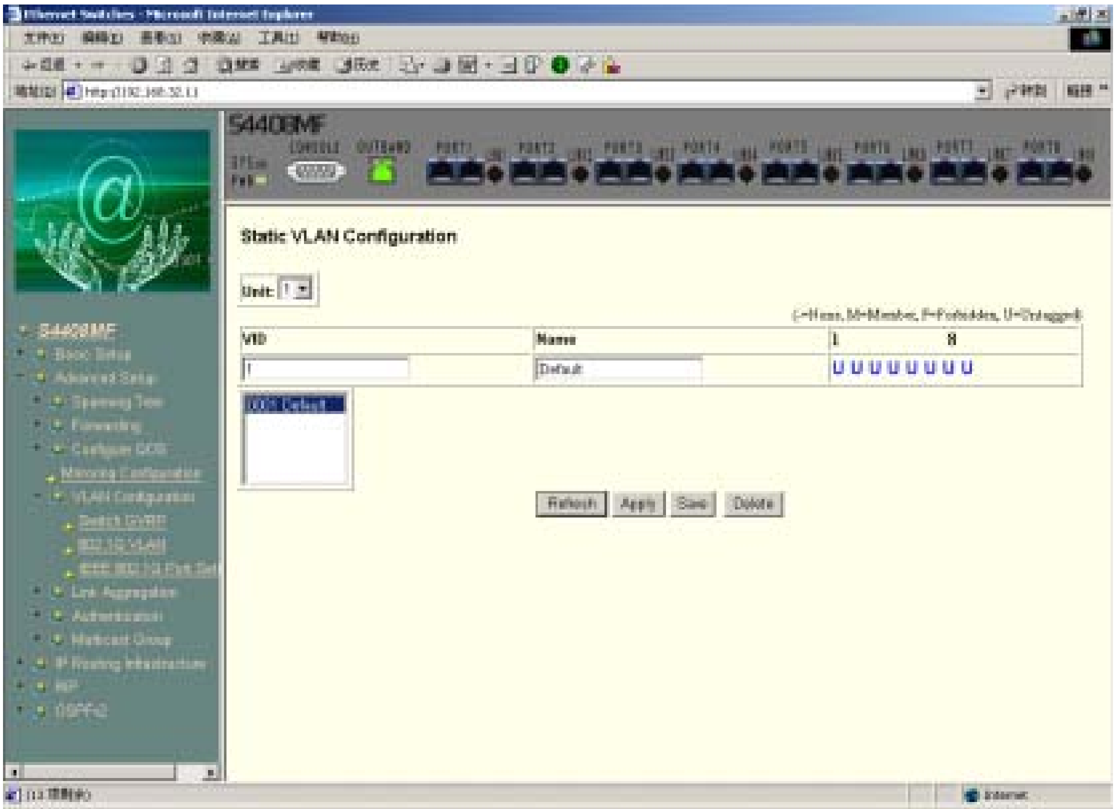


图 6－20 802.1Q VLAN Configuration

交换机保留了一个VLAN, VID = 1，称之为DEFAULT_VLAN。出厂时缺省设置将交换机的所有端口都分配至DEFAULT_VLAN。

上图所示为 802.1Q VLAN 配置界面，在该界面上可以配置哪几个端口归属于哪个 VLAN，不同的 VLAN 用不同的 VID 标识。在 VID 的文本框中输入有效的 ID 号，还可以为该 VLAN 命

名。

在对某个端口进行选择时，会出现“ － ”、“ M”、“ F ”、“ U”四种符号，每个符号代表一定的意义：

－（None）：表示该端口将被禁止成为静态VLAN 的成员，但允许该端口动态地加入任何VLAN。

M（Member）：指端口作为VLAN 中的一个带标记的成员。当一个不带标记的包传输时，包头被改变为包含32 位标记的PVID。当一个带标记包存在时，包头将不改变。

F（Forbidden）：表示该端口将被禁止成为静态VLAN 的成员，而且不允许该端口动态地加入任何VLAN。

U （Untagged）：指端口作为一个不带tag 标记的VLAN 端口。当一个untagged 包通过此端口传输时，此包头保持不便。当一个tagged 包在端口中存在时，此包也将变为一个不带tag 标记的包。

IEEE802.1Q 端口设置（IEEE802.1Q Port Settings）

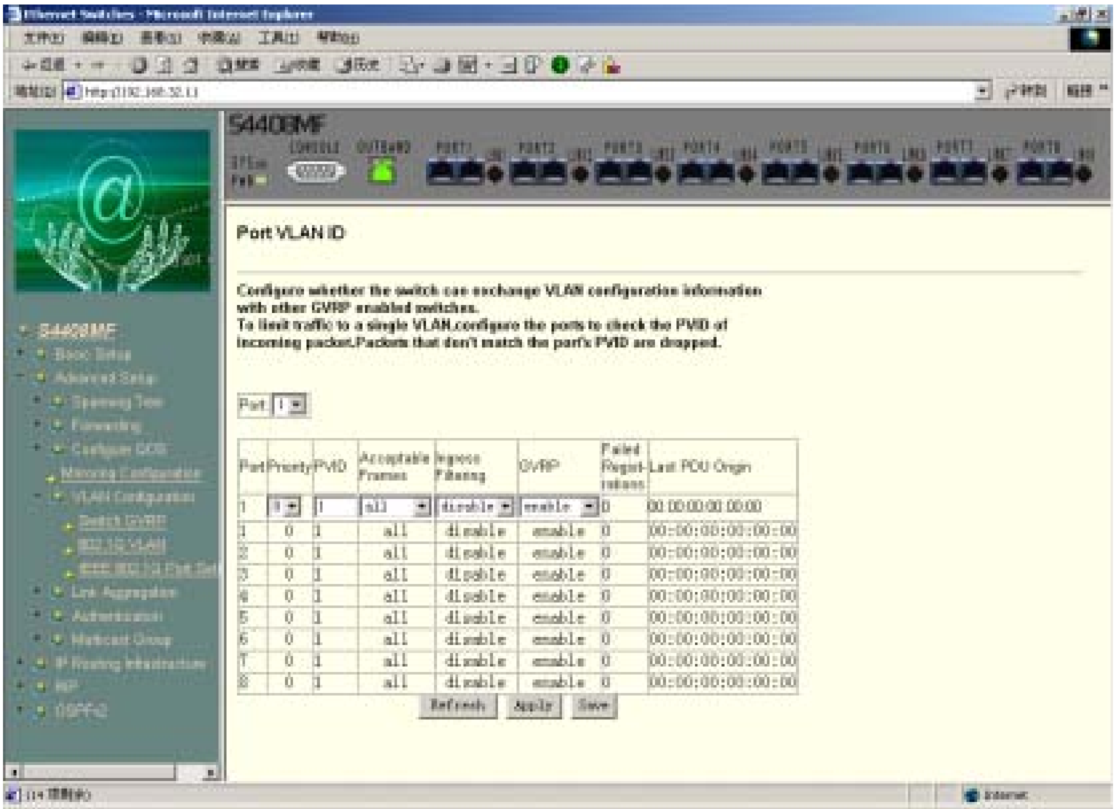


图 6-21 802.1Q Port Settings

一个802.1Q VLAN 端口配置界面如上图所示，各项说明如下：

PVID –PVID 定义了交换机将向哪一个VLAN 转发数据包，以及什么时候数据包会需要转发到另一台交换机的端口上，或者网络中的某个地方。另外，用户也可以定义某个端口同时属于多个VLAN（VIDs），使得它可以接收网络中多个VLAN 的数据包。PVID 和VID 这两个变量用于控

制端口发送和接收VLAN 数据流的能力，而两者之间的区别在于后者还允许信息可以在多个VLAN 间共享。

Ingress Filtering –如果入端口的Ingress Filtering 功能被设置为disable 时，那么，交换机将检查每一个流经该端口的数据包，以决定流经的数据包是否是其所属VLAN 中的成员。然后，做出如下两个动作中的一个：如果该端口所属的VLAN 与数据包中所标记的VLAN 不是同一个，那么，该数据包将被丢弃，反之，将被转发。而如果入端口的Ingress Filtering 功能被设置为enble时，那么，交换机将以通常的方式处理所有流经该端口的数据包。

GVRP – VLAN 组注册协议–将允许端口动态加入一个VLAN 组。

Priority：设置该端口的优先级，同图6-17 QOS的设置是一样的。

6.2.2.6 链路聚合配置（Link Aggregation）

点击配置界面左侧主菜单中的“ Link Aggregation ”，进行链路聚合配置。

链路聚合是由几个端口组合在一起组成的，而且它还可作为一个单一连接来使用，并提供若干单一连接带宽。链路聚合一般用来连接一个或多个带宽需求大的设备，例如连接骨干网络的服务器或服务器群。

注意：S4408MF 允许建立最多6 个链路聚合组，每组包括最多8 个连接（端口）。集合的所有在组中的端口必须是同一个VLAN 中的成员。而且，连接端口必须都是相同速率的，并且都可以配置为全双工。

组中的最小编号端口的配置变成对集合组中所有端口的配置。这个端口被称做组的基础端口，并且包括VLAN 配置的所有配置选项能应用在基础端口被应用的整个链路聚合组中。

负载平衡自动的应用到在集合组中的连接，并且组中的连接失败引起网络通信量被导向组中的保持端口。

注意：生成树协议在交换机层把一个链路聚合像一个单一连接来对待。在端口层，**STP** 将使用基础端口的端口参数来计算端口代价和决定链路聚合组的状态。如果在交换机上配置两个多余的链路聚合组，**STP** 将阻塞一个组，并且**STP** 以同样的方式阻塞一个有多余连接的单一端口。

配置干路端口（**Trunk Port Parameter**）

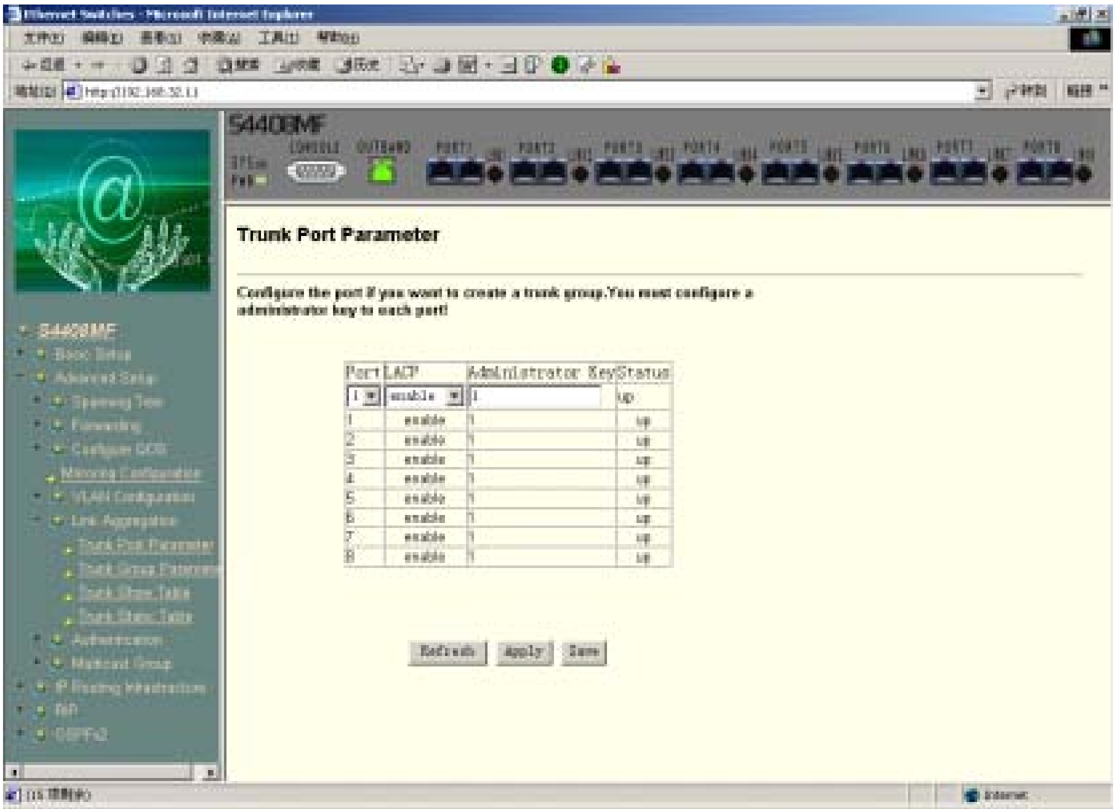


图 6-22 Trunk Port Parameter

干路端口配置界面如上图所示，该页面允许端口是否可以进行动态链路聚合（LACP 为动态链路聚合控制协议）。如果某个端口可以进行动态链路聚合，必须为该端口配置 Administrator key，Administrator key 是一个最大值为 256 的数字。不同设备间具有相同 Administrator key 的端口才可能聚合成一条链路，Administrator key 不同的端口不能聚合在一起。Status 表示该端口的 link 状态，up 或 down。

注意：要使该界面配置生效，必须在图 7－22 配置界面将 LACP 协议使能。

配置干路策略（Trunk Group Parameter）

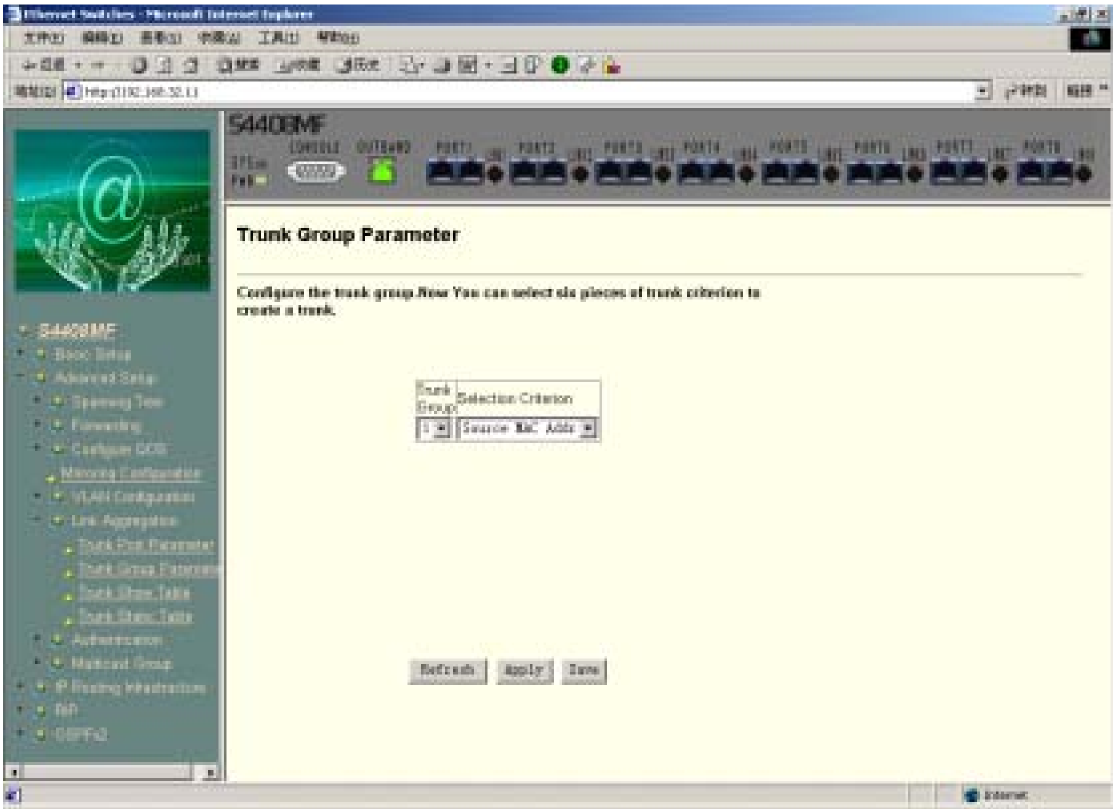


图 6－23 Trunk Group Parameter

上图所示的配置界面列出了端口聚合时进行负荷分担的策略。S4408MF 提供三种策略：

Source MAC Addr：源 MAC 地址；

TPEStination MAC Addr：目的 MAC；

Source & TPESt Ip：源和目的的 IP 地址。

负荷分担策略决定端口聚合后进行报文转发时，报文该发给 TRUNK 成员中的哪个端口。

显示干路组（Trunk Show Table）

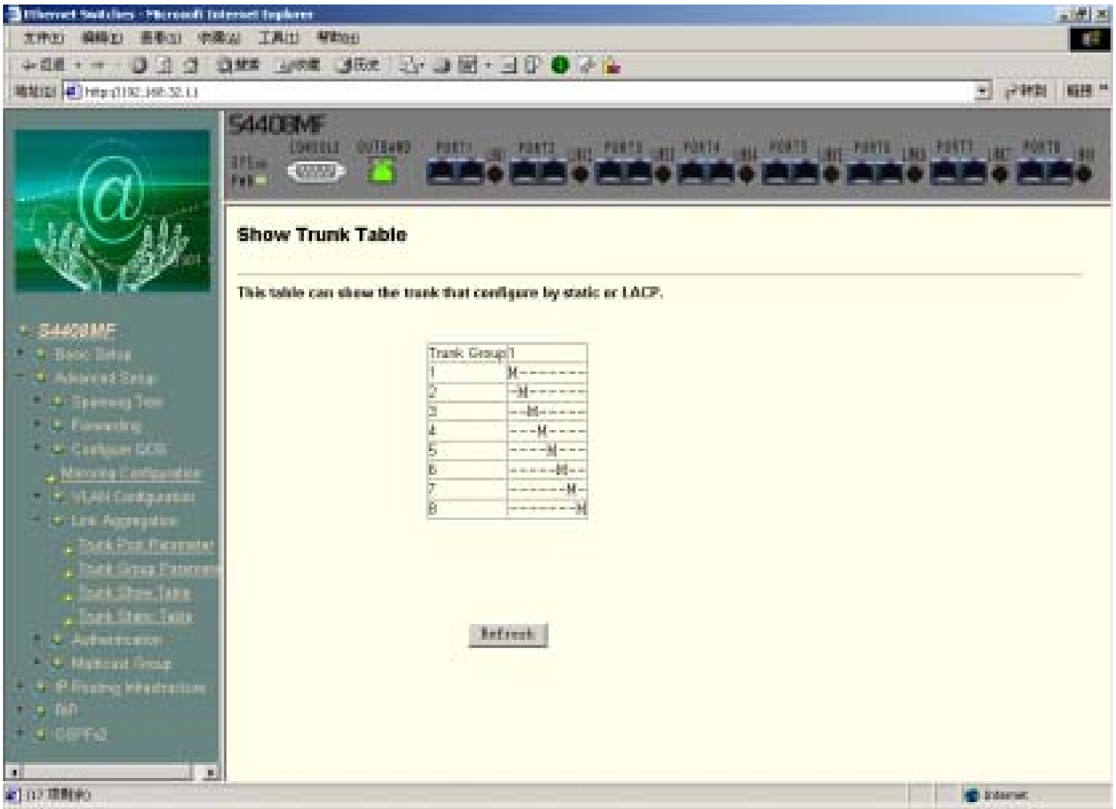


图 6－24 Show Trunk Table

该配置界面显示当前静态 Trunk 的聚合状态，如图中所示：port 1 和 port2 聚合成一个 Trunk，port 3 和 port 4 聚合成一个 Trunk。

配置静态干路（Trunk Static Table）

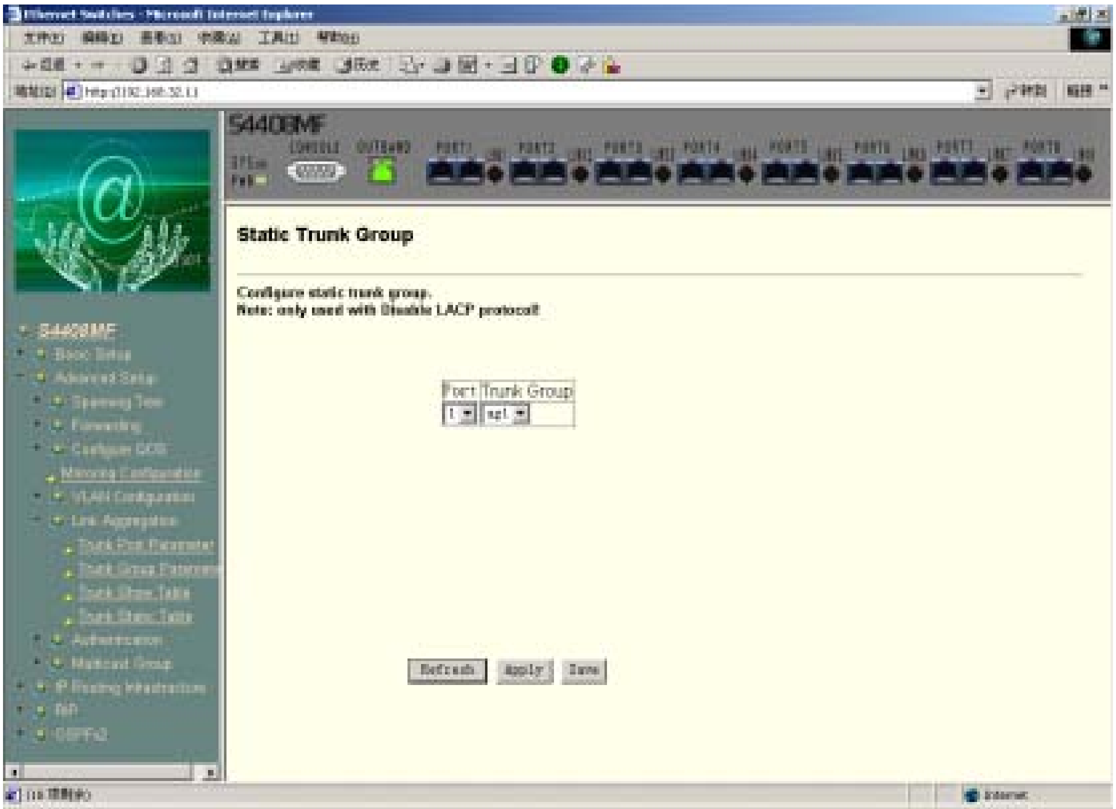


图 6-25 Static Trunk Group

该界面用于配置静态 Trunk，在“ port ”下拉菜单中用户可以选择要聚合的物理端口号，“ Trunk Group ”下拉菜单中用户选择聚合的组标识。

注意：配置静态 Trunk 是全局的 LACP 协议开关必须关闭，在图 7－2 的配置界面操作。

6.2.2.7 认证配置（Authentication）

S4408MF 提供 802.1x 和 WEB+DHCP 两种认证方法，需要对这两种认证方式进行相应配置。WEB 管理界面左侧的“ Authentication ”菜单下有三个配置子菜单，分别是 Radius、8021.x 和 WEB Server 的配置。

注意：DHCP+WEB 的认证同 802.1x 的认证是非此即彼的关系，在同一时刻只能启动其中一种认证方式。

Radius（配置）（Radius Configuration）

点击“ Radius Configuration ”菜单，会显示如下配置页面：

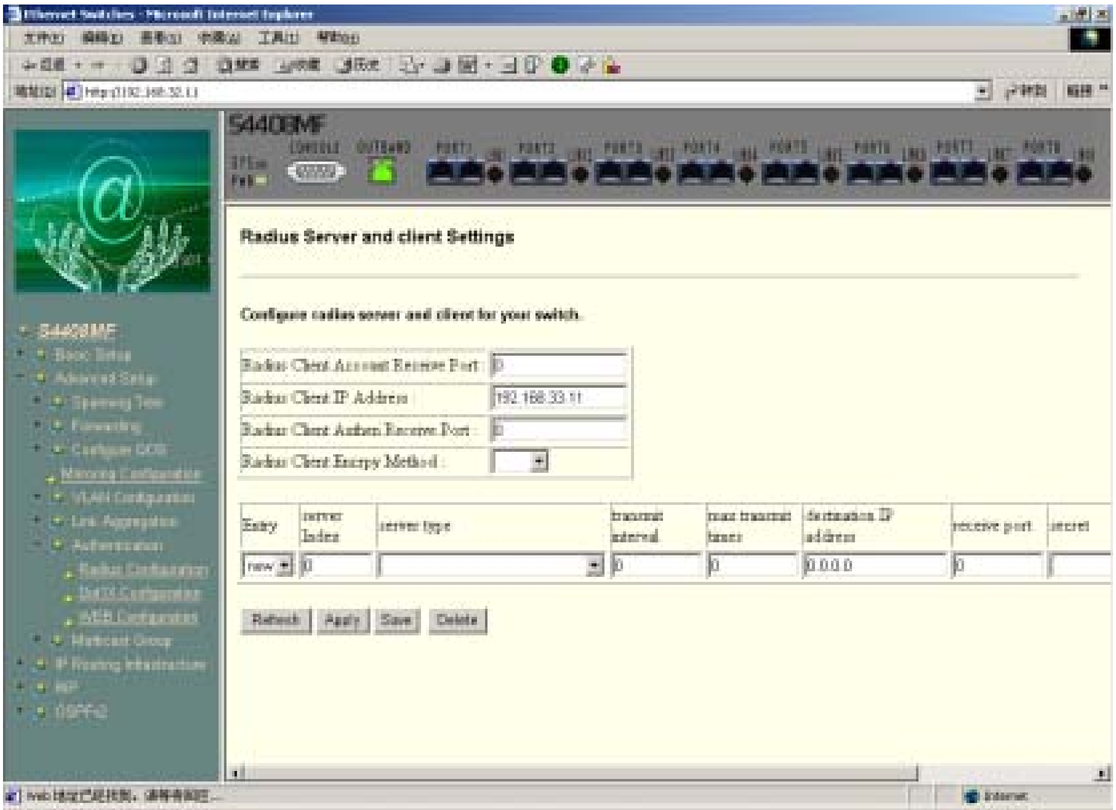


图 6－26 Radius Configuration

该页面完成对 Radius server 和 Radius client 的配置，各项说明如下：

Radius Client Account Receive Port：Radius Client 侧计费报文接收端口号，协议缺省配置为 1813；

Radius Client IP Address：Radius Client 侧的 IP 地址，一般为交换机某个接口的 IP 地址；

Radius Client Authen Receive Port：Radius Client 侧认证报文接收端口号，协议缺省配置为 1812；

Radius Client Encrpy Method：Radius Client 侧密码加密算法，目前支持两种加密算法：CHAP

和 PAP。

表格形式的设置方式用于配置 Radius server，系统支持可以配置多个 Radius Server，最大支持 6 个 Radius Server。

server index：Radius Server 的索引，为 0-5 的数字；

server type：Radius Server 的类型，支持三种 Server 类型 ，认证 Authentication、计费 Accounting 、既可以认证又可以计费 Authentication and Accounting。

transmit interval：Radius client 向 Radius Server 发送请求报文后，在收到 Radius Server 响应前决定重发请求报文的时间间隔，缺省值为 10s。

max transmit times：Radius client 向 Radius Server 发送重传报文的最多重复次数，缺省值为 3。

TPEStination IP address：Radius Server 的 IP 地址；

receive port：Radius Server 接收 radius 报文的端口号，协议缺省的认证请求报文接收端口号为 1812，协议缺省的计费请求报文接收端口号为 1813；

secret：长度为 3-256 的字符串，作为 Radius Server 和 Radius Client 间的共享密钥。

802.1x 配置（Dot1x Configuration）

802.1x 配置界面如下图所示：

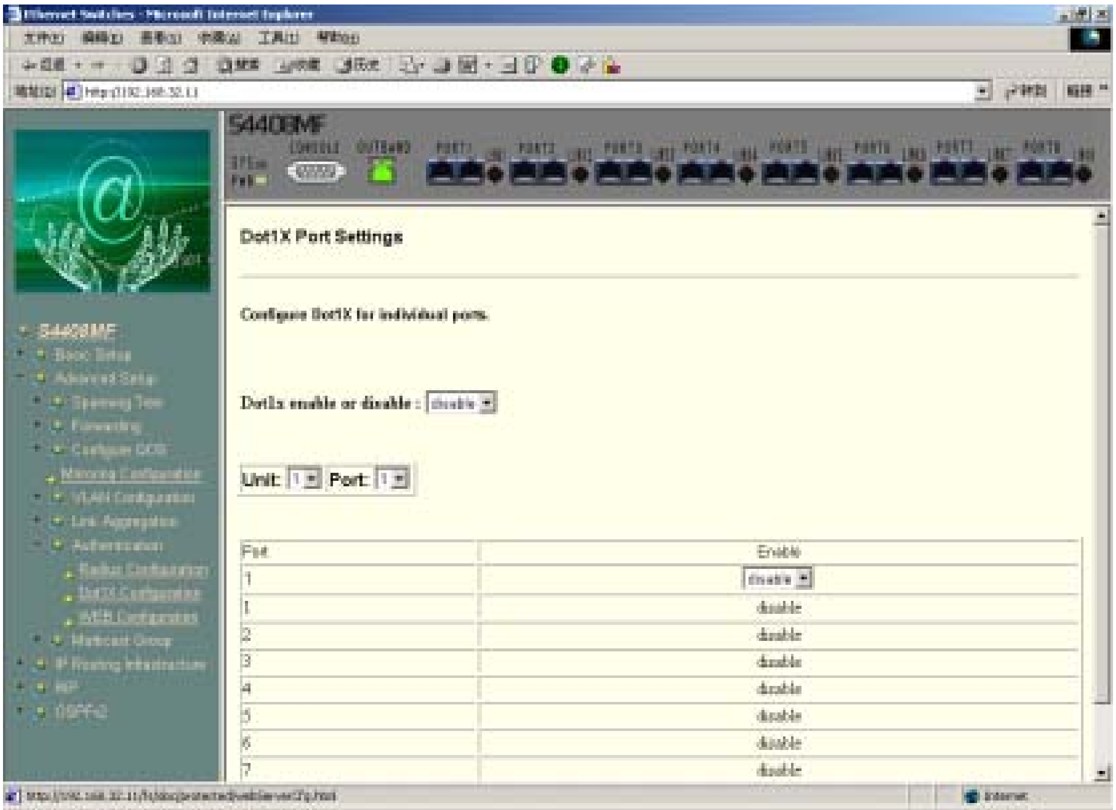


图 6－27 802.1x configuration

Dot1x enable or disable：是否启动 802.1x 认证方式的总的开关：使能或禁止；

针对每个端口号也设置了一个使能禁止开关，目的是用户可灵活控制认证形式：有些端口需要进行认证才能访问 Internet，有些端口不需要通过认证直接可以上网。

WEB SERVER 的配置（WEB Configuration）

该配置界面主要是用于 DHCP+WEB 的认证方式， 需要对以下几项参数进行设置：

AAA module startup：是否启动 AAA 认证鉴权模块；

External Web Server Enable Object：是否需要外部的 Web Server，Enable 表示选择外部的 Web Server，disable 表示 Web Server 内置交换机；只有选择了外部的 Web Server，下面的配置才是有效的。

Radius Client Receive Port：Radius Client 和 Web Server 之间通信时 Radius Client 接收报文的端口号。

WEB Server Receive Port：WEB Server 接收报文的端口号；

WEB Server IP Address：WEB Server 的 IP 地址；

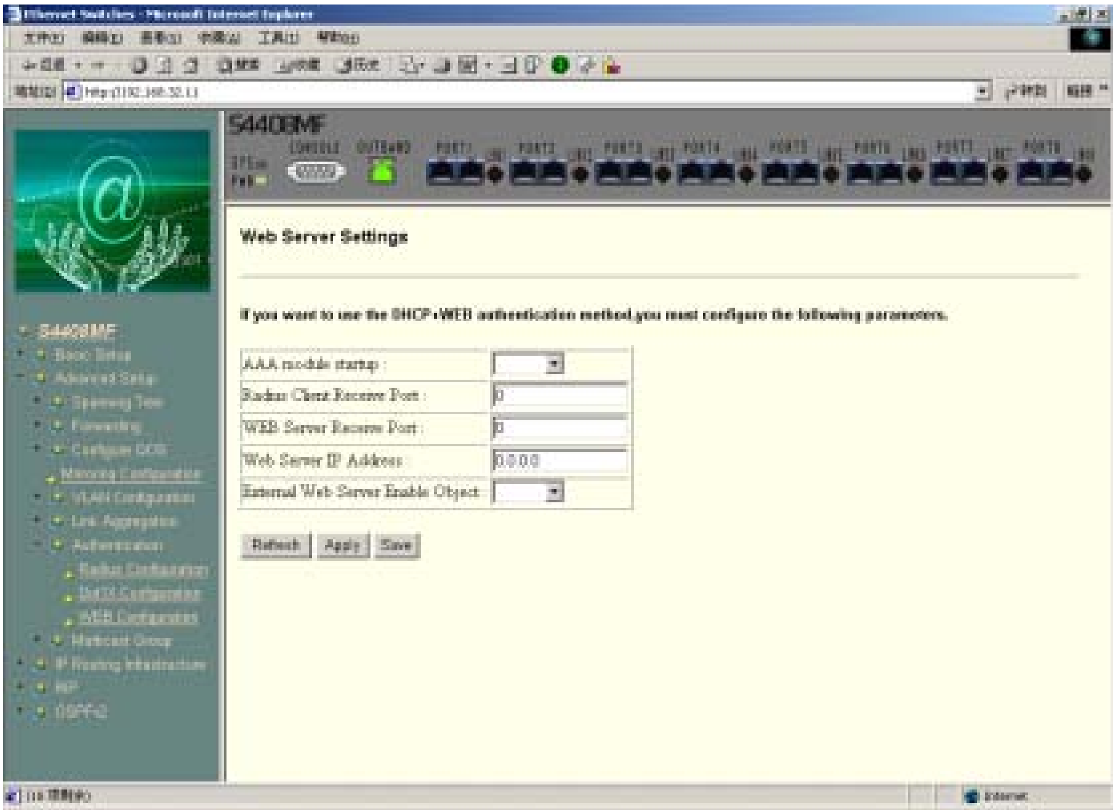


图 6－28 Web Server Settins

注意：WEB Configuration 和 Dot1x Configuration 只能任选其一，两者不能同时配置运行。

6.2.2.8 设置多播组

设置静态多播

通过下面的 web 界面可以设置静态多播。

设置项包括：

vlan id ：一个 vlan 标识。

Mac address：添加一个多播 mac 地址。一个 vlan 域可以有多个多播 mac 地址。

Port：划定属于这个多播组的端口。设定的端口必须是属于选定的 vlan 域。

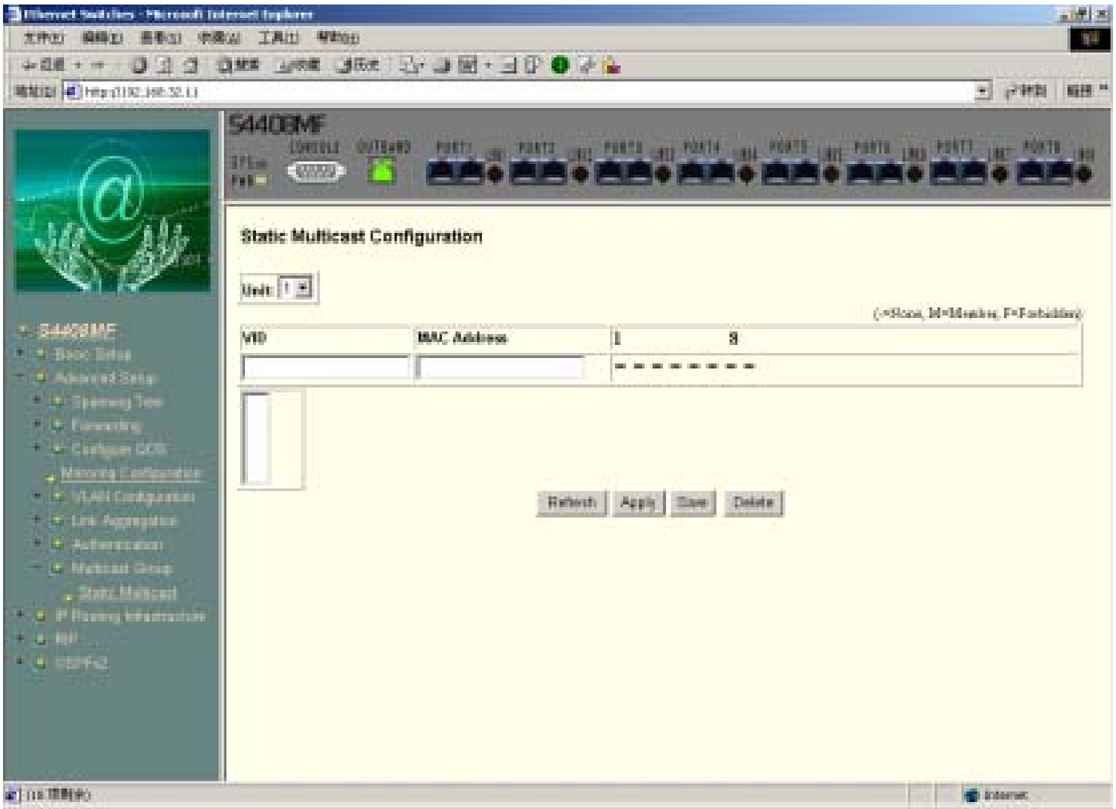


图 6－29 静态多播组设置

6.2.3 IP路由配置（IP Routing infrastructure）

6.2.3.1 子网配置（Subnets）

子网配置界面如图 6－30 所示，需要对以下参数进行配置后，按“ Apply ”按钮使配置生效。

IF：选择子网的 IP 接口 sw0－sw15，每个 sw0 代表一个 Supervlan。

Destination IP Address：该子网网段接口的 IP 地址，既 Supervlan 接口的 IP 地址；

Subnet Mask：该子网网段的网络掩码；

Description：对该子网的描述，为一字符串；

Status：该子网的状态，是 " Active " 还是 " Notready "；

Subsw BitMaps：表示 256 个 Subvlan，一个 Supervlan 可以包含多个 Subvlan，所包含的 Subvlan 通过点击符号 " — " 变为符号 " M " 来表示。图 7—30 所示的 Supervlan sw0 包含 1、3、5 三个 Subvlan。

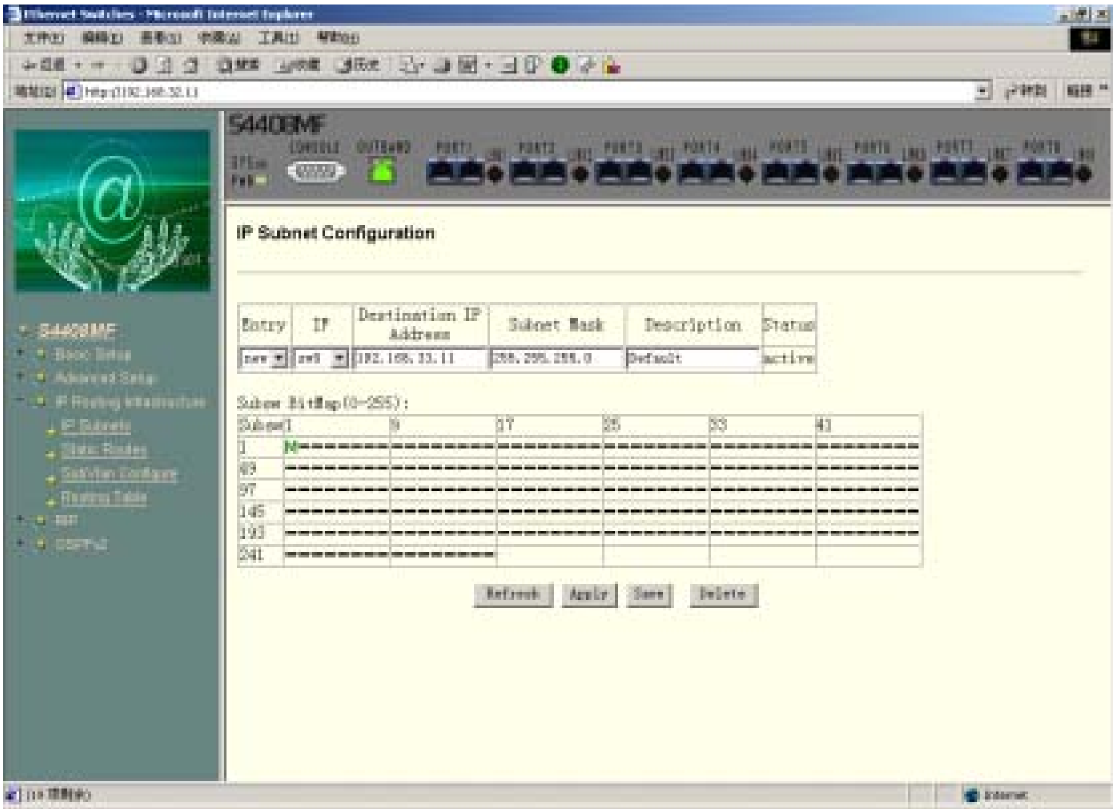


图 6—30 IP Subnet Configuration

6.2.3.2 配置静态路由（Static Routes）

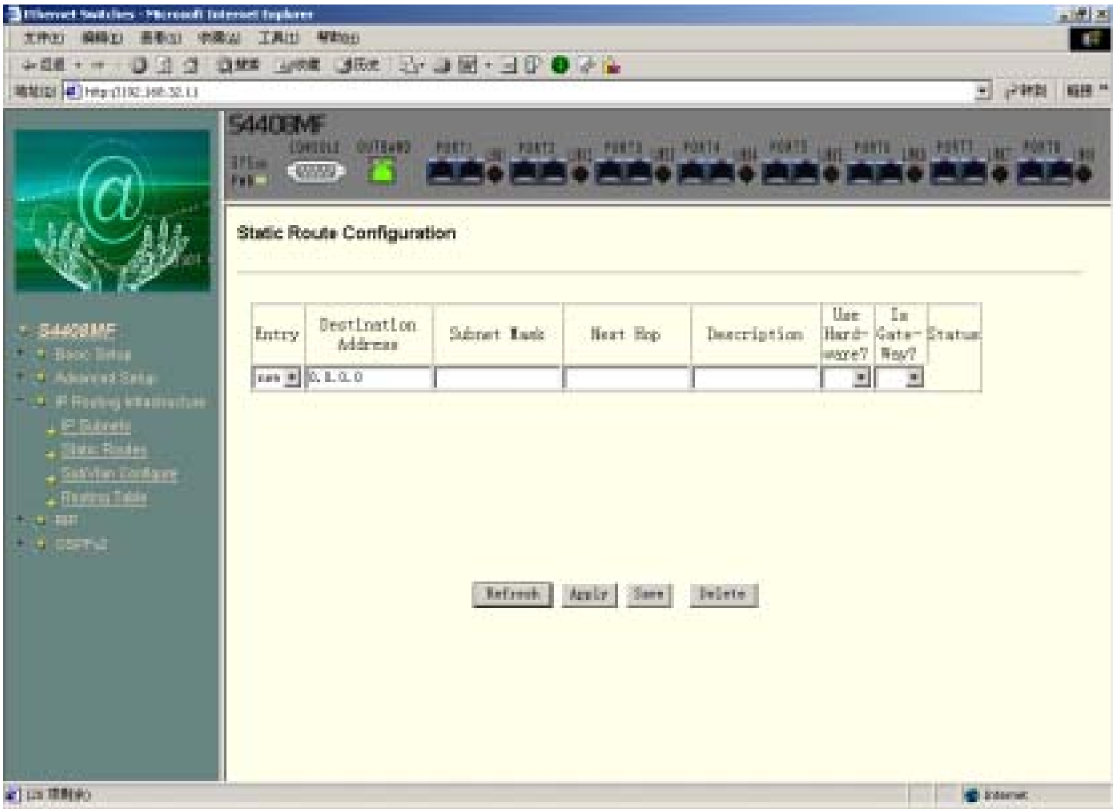


图 6-31 Static Route Configuration

静态配置页面如上图所示，用户可以操作该页面来添加静态路由。

Destination Address：路由器或网关的 IP 地址，点分十进制方式表示；

Subnet Mask：路由器 IP 地址的子网掩码，点分十进制方式表示；

Next Hop：去往该静态路由的下一跳的 IP 地址，往往为交换机的 IP 接口地址，点分十进制方式

表示；

Description：对该静态路由的描述，为一字符串；

Use Hard-ware：选择 “ yes ” 或 “ no ” 来决定该静态路由配置信息是否固化到硬件中；

Is Gate- Way：选择 “ yes ” 或 “ no ” 来决定该静态路由配置信息是否作为网关使用；

Status：所配置的静态路由的状态，是 “ Active ” 还是 “ Notready ”。

6.2.3.3 SubVLAN的配置（SubVLAN Configuration）

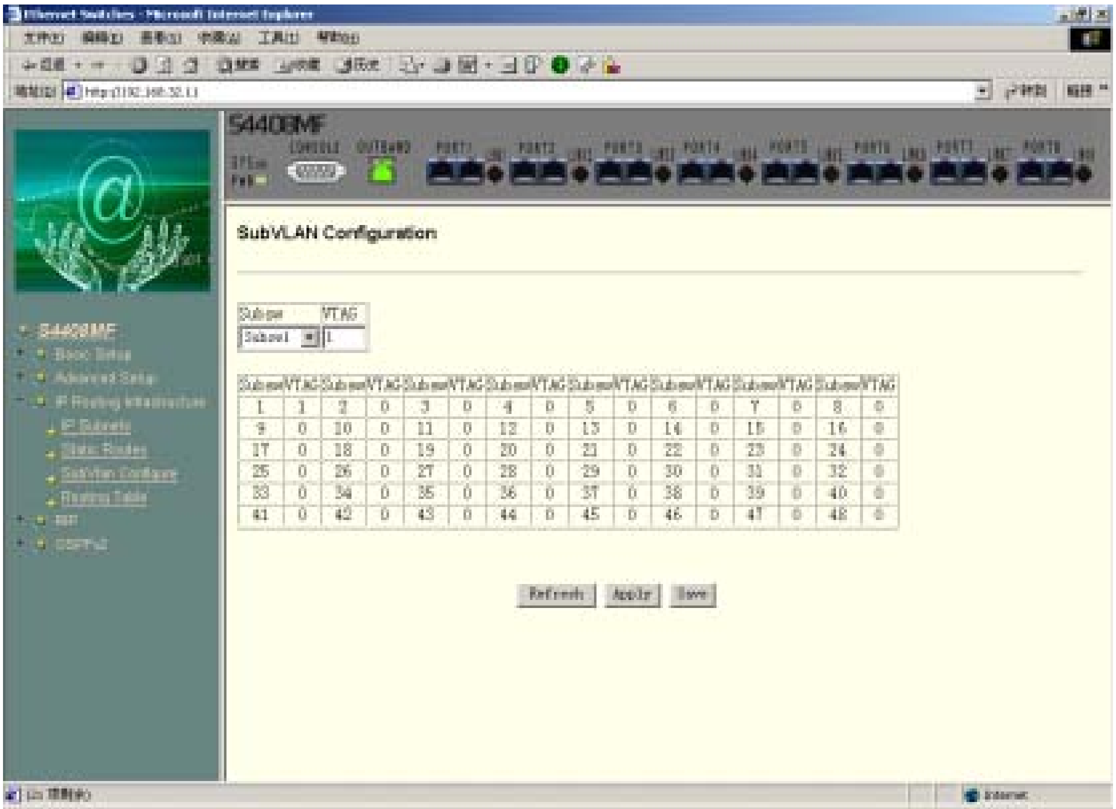


图 6－32 SubVLAN Configuration

该界面主要完成 subVlan 和 VID 的绑定关系的配置。在“ Subsw ”的下拉框中，选择相应的 Subswx 表示 subvlan，在 VTAG 的下拉框中填写 subvlan 的 VID。表格显示的是 subVlan 和 VID 的对应关系。

注意：配置该界面的前提是图 7-21 所示的 802.1Q VLAN 已经配置。

6.2.3.4 显示路由表（Routing Table）

图 6-33 显示的是所有路由表的信息，包括静态路由和动态路由信息。

TPESt Addr：路由的目的 IP 地址，以点分十进制表示；

Mask：路由网段子网掩码，以点分十进制表示；

Next Hop：去往该静态路由的下一跳的 IP 地址，往往为交换机的 IP 接口地址，点分十进制方式表示；

Next Mac：下一跳的 MAC 地址；

ifIndex：网络接口的索引值；

Type：和本交换机关联的路由类型，是直接路由“ direct ”还是间接路由“ indirect ”；

Protocol：该路由信息被学习到的路由机制，既该路由信息是通过何种协议获取的。“ other ”表示无协议；“ local ”表示路由信息是本地手工配置的；“ icmp ”指示该路由信息由 ICMP 协议间接得到；“ rip ”和“ ospf ”是另外两种路由协议。

Age：该路由的老化时间，只对动态路由有效，静态路由不进行老化 处理；

Metric1：交换机到该路由器的路径开销，该值是由“ protocol ”指定的路由协议来决定的。

In HW：表示该路由信息是否在硬件路由表中；

Is Static：表示该路由信息是静态的还是动态的。动态路由信息由 RIP 或 OSPF 协议创建。

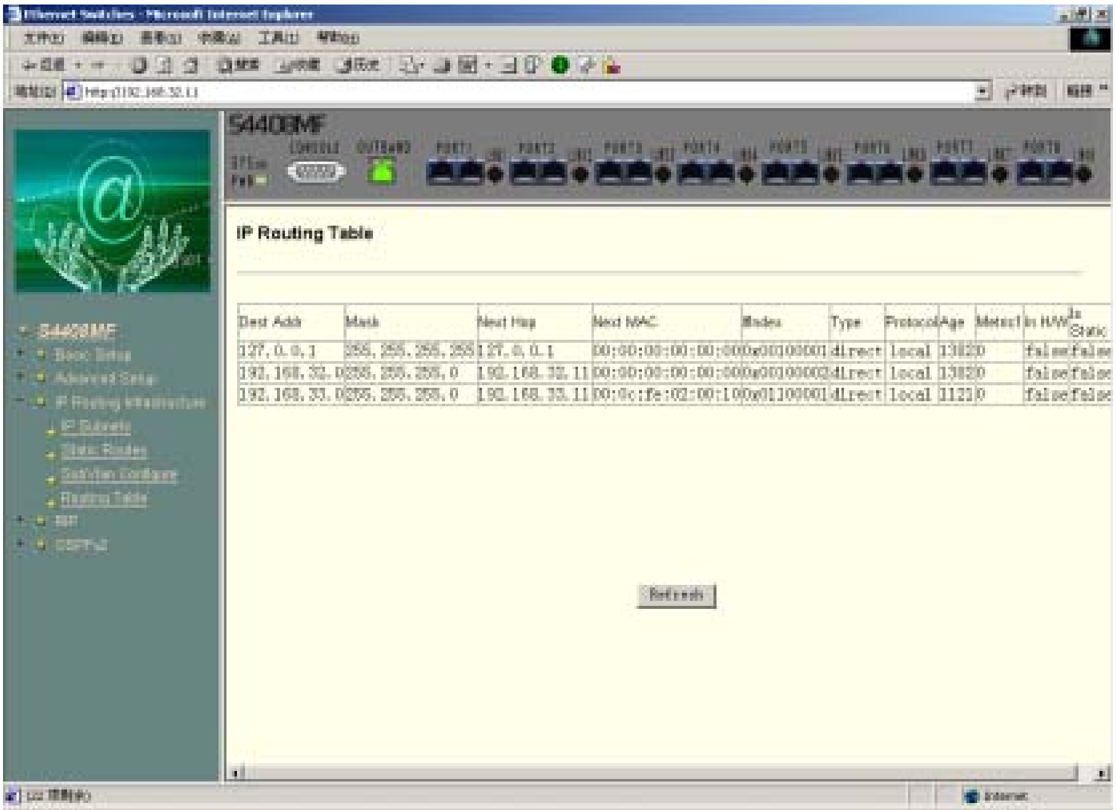


图 6－33 IP Routing Table

6.2.4 RIP协议（RIP）

配置界面左侧的 “ RIP ” 菜单包含 RIP 协议配置和 RIP 信息统计两个子菜单。

6.2.4.1 RIP 配置（RIP Configuration）

图 6-34 所示界面完成对 RIP 协议的配置，包括下述参数：

IP Address：交换机网络接口的 IP 地址，该项在此不可配，其配置是在图 6-29 子网配置界面实现的。本界面 IP Address 只是 MIB 库的索引值。

Authentication Type：RIP 协议的验证方法，用于对 Authentication Key 进行验证。包含三种验证算法：

noAuthenticaion：对 RIP 协议报文不进行验证；

simplePassword：简单密码验证方法；

md5：md5 验证方法。

Authentication Key ID：用于标识 Authentication Key 的标识符，1－255 内的整数值。

Authentication Key：验证密钥，一个长度为 0-16 的八位位组字符串。Authentication Type 和 Authentication Key 一起完成对 RIP 协议报文的鉴权验证。只用两台设备设置了相同的 Authentication Type 和 Authentication Key，它们之间互通的 RIP 报文才能通过验证，才能进行 RIP 协议的互通。

Send Type：发送 RIP 报文的类型，包括：

doNotSend：无发送动作；

ripVersion1：RIPV1 版本兼容 RFC1058;

rip1Compatible：RFC1058 的路由规则下支持广播 RIP－2；

ripVersion2：支持组播 RIP－2；

Receive Type：接收 RIP 报文的类型，包括：

rip1：接收 RIP 版本 1 的报文；

rip2：接收 RIP 版本 2 的报文；

rip1OrRip2：RIP 版本 1 的报文和 RIP 版本 2 的报文都可以接收；

doNotRecieve：不接收 RIP 报文。

Default Metric：指定该网络接口（IP 地址决定）的距离向量度量值的大小。

注意：

1. **配置 RIP 协议时，必须确定 RIP 协议已经使能，在图 7-2 配置界面路由协议选项进行 RIP 协议的使能/禁止动作。**
2. **下图的操作界面只能用于修改或者显示设置的结果，不能创建新的表项，在添加了新的 supervlan 项时，在下图的显示中，会多一个对应的项。**

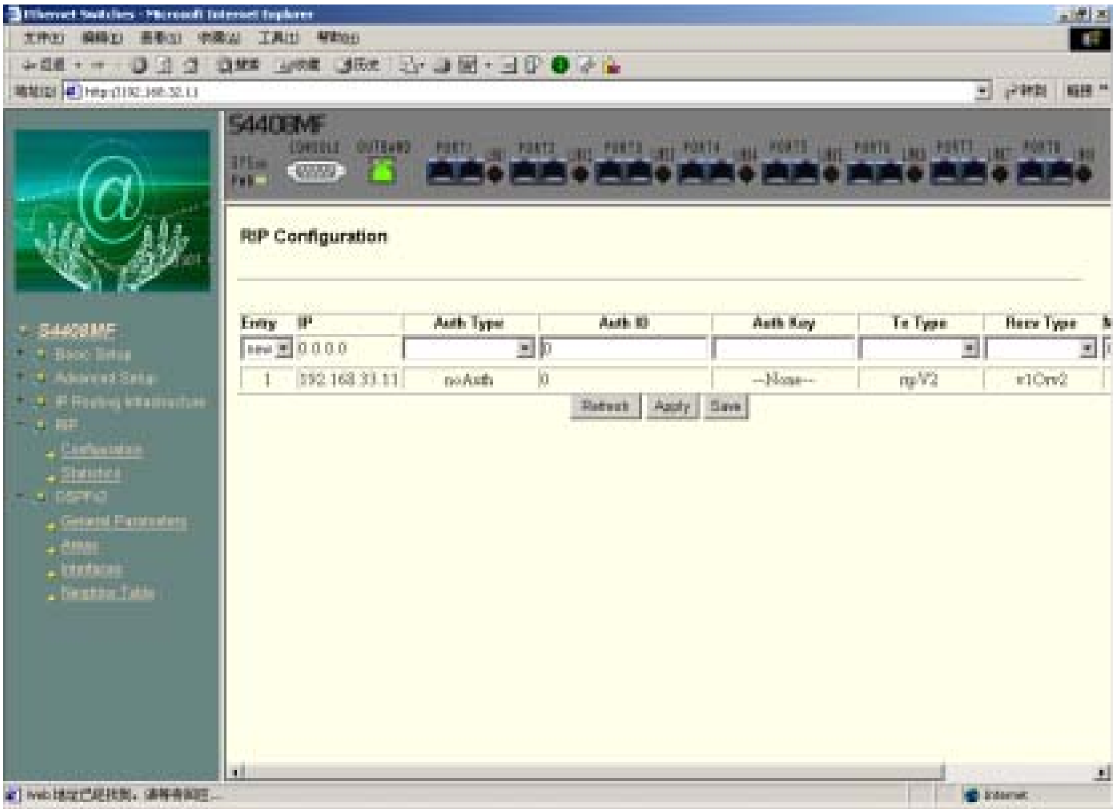


图 6－34 RIP Configuration

6.2.4.2 RIP信息统计（RIP Statistics）

图 6-35 所示界面统计了 RIP 的一些信息，包括下述 MIB 变量：

Route Changes：本次系统启动以来路由改变的次数；

Queries：对来自其它系统的 RIP 查询的响应次数；

IP Address 交换机网络接口的 IP 地址,其配置是在图 6-30 子网配置界面实现的。本界面 IP Address 用于标识网络接口。

Bad Packets Received：该接口接收到的坏的该被抛弃的 RIP 响应包；

Bad Routes Received：无效的该被忽略的路由次数；

Updates Sent：在该接口通过触发刷新机制发送的 RIP 数据包的个数。

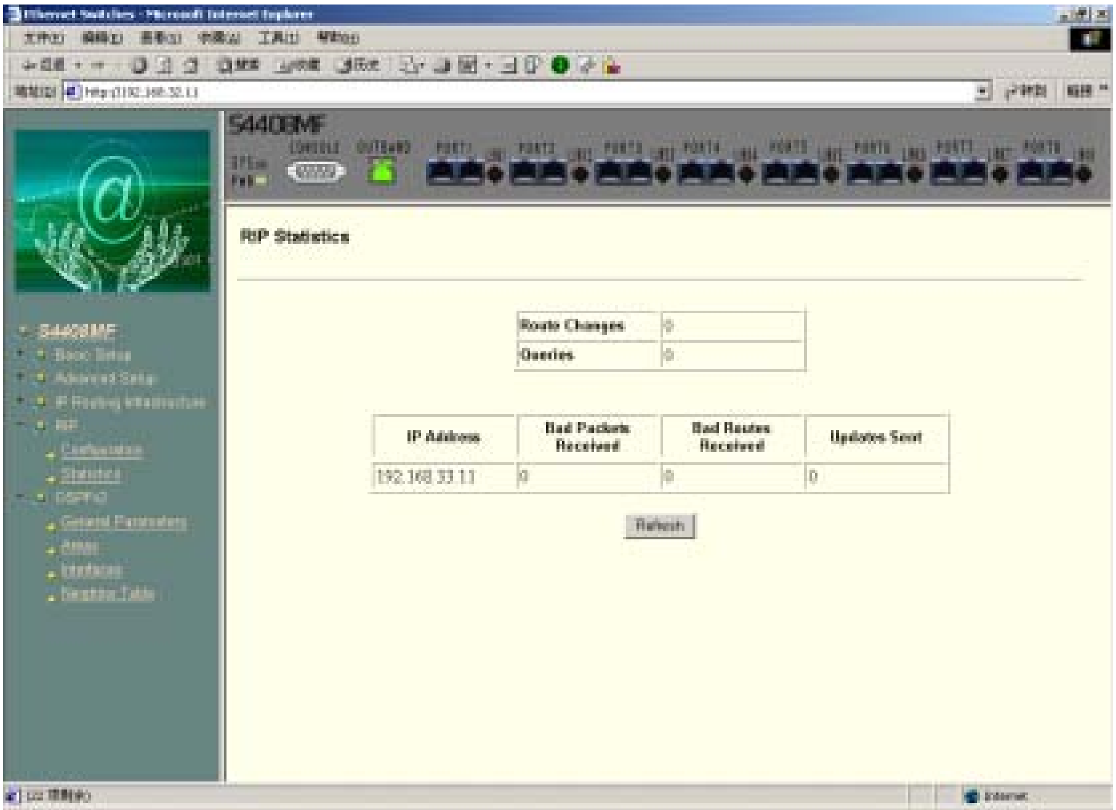


图 6－35 RIP Statistics

6.2.5 OSPFV2协议（OSPFv2）

点击配置界面左侧的“ OSPFv2 ”，完成对 OSPF 协议的配置操作。

6.2.5.1 OSPF一般参数（OSPF General Paramters）

下图为 OSPF 协议一般参数的配置和显示界面，各参数描述如下：

Router ID：路由器标识符，以点分十进制方式表示；

Admin Status：该路由器的管理状态；

Version：OSPF 路由协议的版本号，**目前只支持版本 2**；

Area Border Router：所配置的路由器是否为区域边界路由器；

AS Border Router：所配置的路由器是否为自治域边界路由器；

External LSA Count：外部链路状态广播数据包的数目；

External LSA Checksum Sum：外部链路状态广播数据包的校验和；

TOS Support：是否支持 TOS（type of service）；

New LSA Received：接收到的新的链路状态广播数据包的数量；

External LSDB Limit：链路状态数据库的个数，－1 表示对数据库个数无限制；

Multicast Extensions：是否支持组播扩展，S4408MF 交换机目前不支持该功能；

Exit Overflow Interval：链路状态数据库溢出后停止接收链路状态广播数据包到链路状态数据库恢复重新开始接收链路状态广播数据包的时间间隔；

Demand Extension Support：是否支持需求扩展，**S4408MF 交换机目前不支持该功能。**

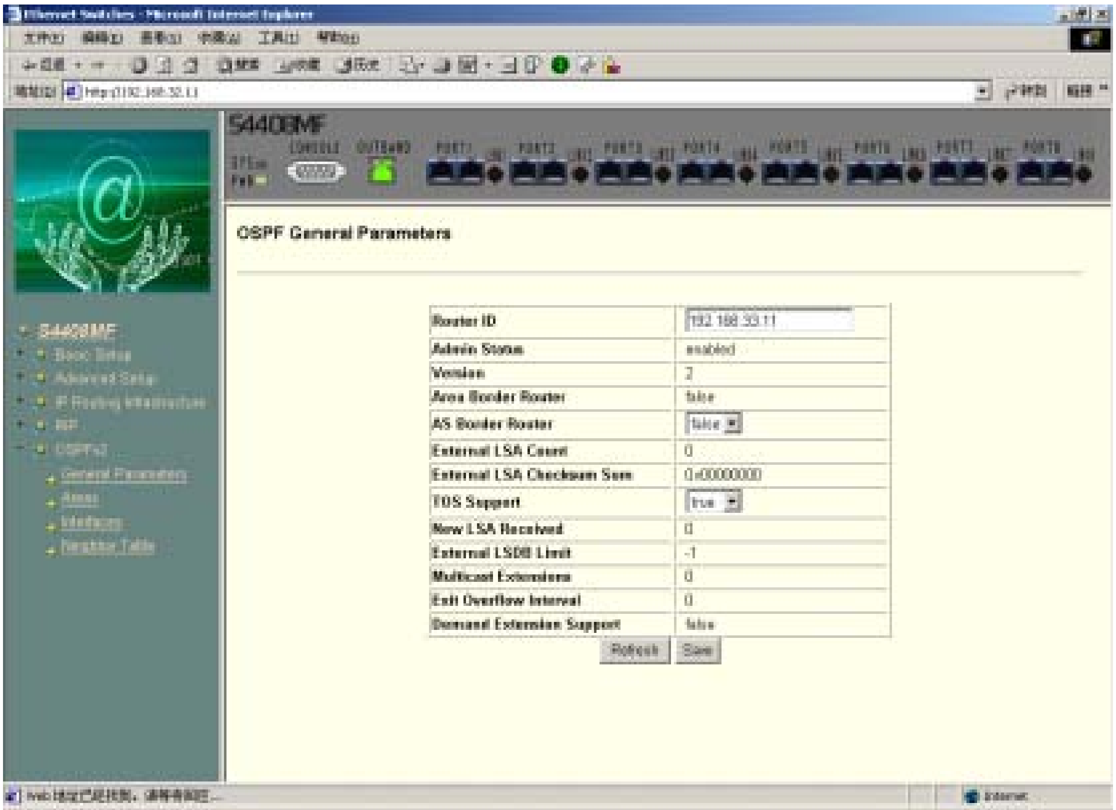


图 6－36 OSPF General Parameters

6.2.5.2 OSPF区域配置（Areas）

图 6-37 所示为 OSPF 区域配置界面，配置内容如下所示：

Area ID：用于标识区域的标识符，以点分十进制方式表示；

AS Option：区域自治系统的选择，支持三种模式：

importNoExternal: Must have a default route,does not support externals、importExternal:

Must have a default route, does support externals

importNssa: Must have a default route, supports limited externals。

(NSSA:Not-So-Stubby_Area RFC1587)

Route Table Updates：该区域路由表更新次数；

Border Routers：该区域边界路由器的数目；

AS Border Routers：该区域中自治域边界路由器的数目；

LSA Count：该区域中链路状态广播数据包的数目；

LSA Checksum Sum：: 该区域中链路状态广播数据包的校验和；

Summary Option：链路状态广播的摘要选择；

Status：区域状态

注意：

1. **在配置 OSPF 协议时，必须确定 OSPF 协议已经使能，在图 6-2 配置界面路由协议选项进行 OSPF 协议的使能/禁止动作。**
2. **如果设置的 area 已经在使用，不可以使用删除命令。**

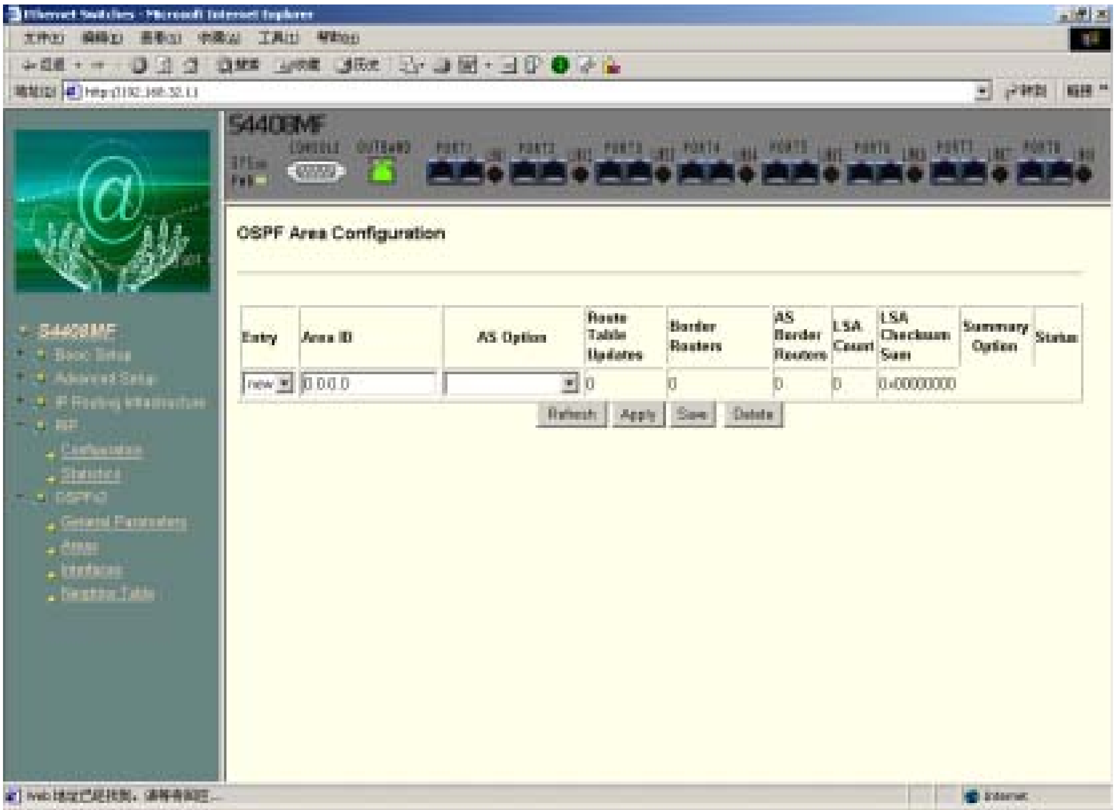


图 6－37 OSPF Area Configuration

6.2.5.3 OSPF接口配置（Interfaces）

OSPF 接口配置界面完成对接口相关参数的配置，界面中各项参数说明如下：

IP Address 交换机网络接口的 IP 地址，其配置是在图 7-30 子网配置界面实现的。本界面 IP Address 用于标识网络接口；

Area ID：用于标识网络接口区域的标识符，以点分十进制方式表示，必须和图 7-37 所示的配置

界面相同；

IFType：该接口类型，支持四种类型，既 broadcast，nbma，pointToPoint，pointToMultipoint；

Admin Status：该接口是否使能 OSPF 协议，既接口的协议状态；;

Priority (1-255)：该接口的优先级，数值越高，表明优先级越高。该优先级在选举指派路由器时使用。

Transit Delay (0-3600)：接口传输延迟，从该接口发送报文的估计的延迟时间，单位为秒；缺省值为 1S；

Retransmit Interval：链路状态广播报文从该接口发送出去后到没收到相应响应报文决定重传该报文的时间间隔，缺省值为 5S；

Hello Interval (1-65535)：该接口定时发送呼叫报文的时间间隔，单位为秒，缺省值为 10S；

Router Dead Time：如果在该时间内该接口没有没收收到某个路由器的呼叫报文，则认为路由器已经死掉，单位为秒；缺省值为 40S；

Poll Interval：NBMA 网络下路由器的轮循间隔，认为对方已经 INACTIVE。单位为秒；缺省值为 120S。

State：接口状态，包括下列状态：

down，

loopback，

waiting，

pointToPoint，

TPESignatedRouter，

backupTPESignatedRouter，

otherTPESignatedRoute。

TPESignated Router：指派的路由器 IP 地址，以点分十进制方式表示；

Backup TPESignated Router：备份指派路由器的 IP 地址，以点分十进制方式表示；

Events：该接口曾发生的事件次数；

Authentication Type：OSPF 协议的验证方法，用于对 Authentication Key 进行验证。包含三种验证算法：

none：对 OSPF 协议报文不进行验证；

simplePassword：简单密码验证方法；

md5：md5 验证方法。

Authentication Key：验证密钥，一个长度为 0-256 的八位位组字符串。Authentication Type 和 Authentication Key 一起完成对 OSPF 协议报文的鉴权验证。只用两台设备设置了相同的 Authentication Type 和 Authentication Key，它们之间互通的 OSPF 报文才能通过验证，才能进行 OSPF 协议的互通

Multicast Forwarding：指示该接口是否能转发组播报文，有三种选择：

Blocked：不进行组播转发；

Multicast：使用组播地址进行组播转发；

Unicast：单播转发到每个 OSPF 邻居。

Demand Support：BOOL 类型变量，决定是否支持需求电路。**S4408MF 交换机不支持此功能；**

Status：该行表格状态。

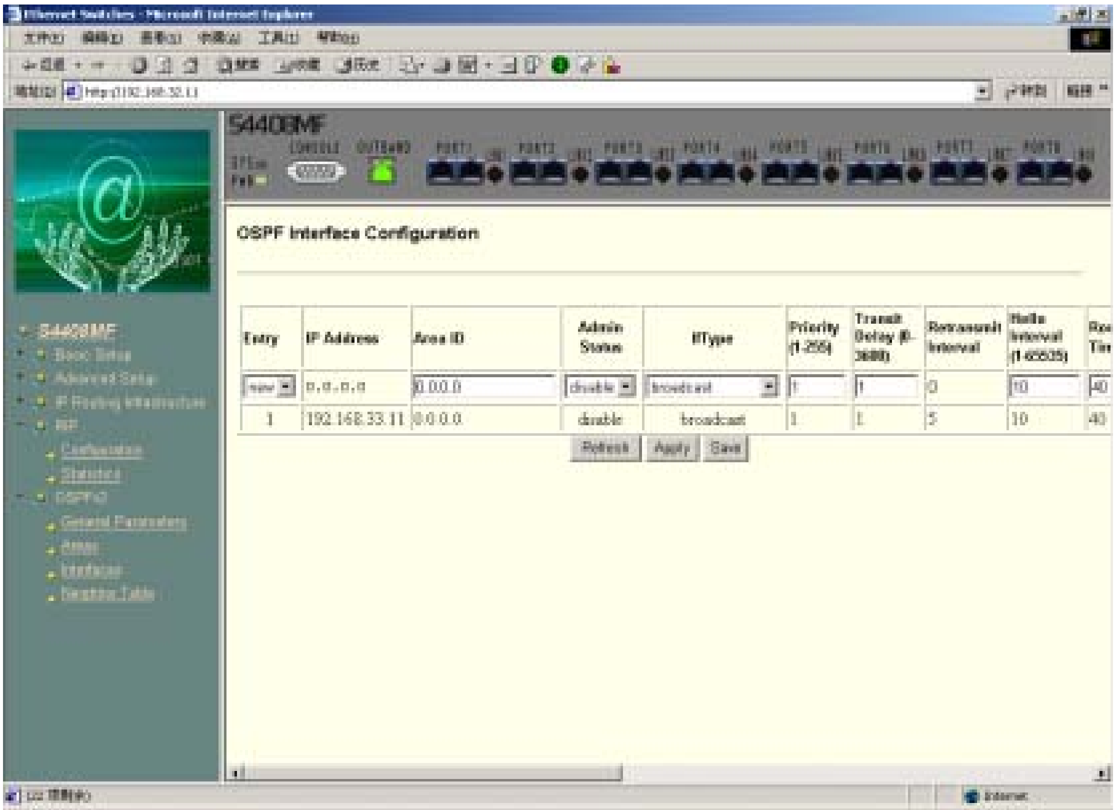


图 6－38 OSPF Interface Configuration

6.2.5.4 邻居路由信息（Neighbor Table）

图 7-39 所示界面显示了通过 OSPF 协议获取的邻居路由器基本信息，包括：

IP Address：邻居路由器的 IP 地址，以点分十进制方式表示；

Router ID：邻居路由器的标识 ID；

Options：通过比特屏蔽来标识邻居的可选域，不同的比特置 1 或 0 有不同意义；

Priority：邻居路由器的优先级，优先级越高，越可能成为指派路由器；

State：本设备同邻居设备的关系状态，有可能的 8 种状态：

down

attempt

init

two Way

exchangeStart

exchange

loading

full

Events：邻居路由器状态改变次数或错误事件发生次数；

RetransQLen：重传队列的长度；

Status： 邻居设备的状态；

Permanence：用来指明邻居信息是如何获知的，有两种方法：

dynamic：通过 OSPF 协议动态获取；

permanent：通过配置的地址获取。

Hello Suppressed：BOOL 类型变量，表示邻居路由器是否抑制 HELLO 报文的发送。

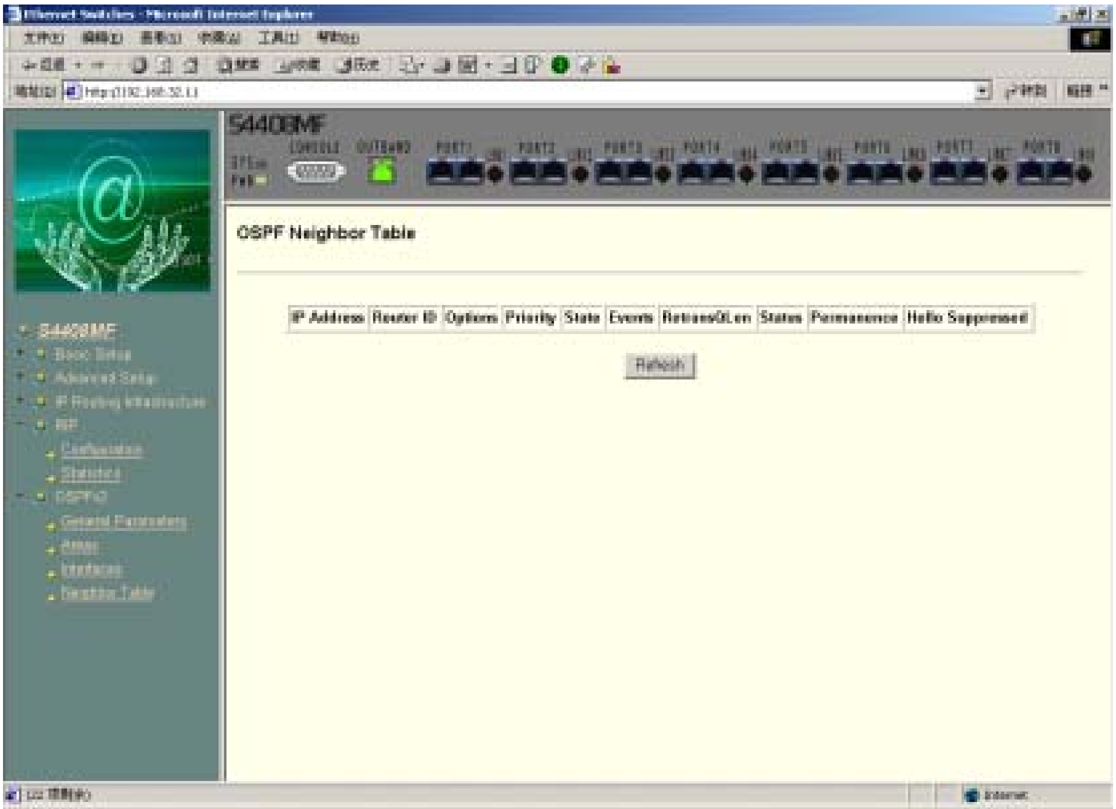


图 6—39 OSPF Neighbor Table

第七章 用户常见问题

问题	回答
加电时所有指示灯均不亮	可能是电源连接错误或供电不正常，请检查电源线和插座
指示灯闪烁	可能是网线接线不标准,网线过长超出允许范围 请更换或重做网线
网络能通，但传输速度变慢，有丢包现象	可能交换机与网络终端以太网口工作模式不匹配,请设置以太网口工作模式使其匹配或将其设为自适应工作模式
正常工作一段时间后停止 工作，而电源不正常,过热	请仔细检查以下两个方面： 1.检查电源是否有接触不良、电压过低或过高。 2.检查周围环境，通风孔是否畅通，交换机风扇是否工作正常
不能通过 Telnet 访问系统	可能是网络连接不正确，IP 地址未配置，请检查网络连接 通过串口访问系统，正确配置 IP 地址 或者是您还没有创建超级用户，创建方法请见(supervlan)
Switch(VLAN)#reset-------无法清空当前的 VLAN 配置	该命令用于清空当前未保存生效的 vlan 配置，即已使用配置了命令，但未用 apply 保存生效时。
配置超级用户的 acceslevel 为 15 时为管理级别，普通用户的 acceslevel 为多少？	S4408MF 用户 accesslevel 为 0—15,除了 15 为管理员级别，其它由用户自定义。